Bürgerrechte & Polizei

CILIP 71
Nr. 1/2002

Überwachung neuer Kommunikationstechnologien

Rasterfahndung
V-Leute und NPD-Verbot
Anti-Terror-Gesetz in Kraft
Tödlicher Brechmitteleinsatz

Editorial

von Heiner Busch

Junge, gutaussehende und wohlhabende Freizeitmenschen tummeln sich mit ihren Handys in der freien Natur. Wichtige Träger von Verantwortung und Designerklamotten sind permanent erreichbar. Boris Bekker ist im Internet „drin". Glaubt man der Werbung der Anbieterfirmen, dann ist die schöne, neue, allseitig und grenzenlos kommunizierende Welt voll von nützlichen Informationen und spaßiger Unterhaltung. Die Kluft zwischen dieser Wunderwelt und den Warnungen von Polizei, Geheimdiensten und SicherheitspolitikerInnen könnte größer nicht sein. Die grenzenlose Freiheit der Kommunikation verwandelt sich im Handumdrehen in einen Abgrund von Kinderschändern, Drogenhändlern, Terroristen und sonstigen Staatsfeinden. Dank modernster Technik laufen die Halunken den staatlichen Ordnungshütern wieder einmal davon.

Die Lösung, die letztere vorschlagen, ist im Grundsatz nicht neu. Sie lautet: Es dürfe keine „rechtsfreien Räume" geben. Jede Kommunikation müsse prinzipiell überwachbar sein. Neue Kommunikationstechnologien dürften nicht zugelassen werden, wenn sie keine Zugangsmöglichkeiten für die Polizeien und Geheimdienste böten. Damit das gewährleistet wird, arbeiten Industrie und Sicherheitsbehörden in geheimen Gremien zusammen und entwickeln technische Schnittstellen. Die Zusammenarbeit lohnt sich auch für die Unternehmen, denn Überwachungstechnik hat ihren Preis.

Der Druck, den das Sicherheitskartell – sprich: die Behörden und ihre Politiker – im vergangenen Jahrzehnt erzeugt hat, hat sich offensichtlich gelohnt. Die Klagen aus der ersten Hälfte des letzten Jahrzehnts, dass Mobiltelefone nicht oder nur mit großem Aufwand zu belauschen seien, sind längst verstummt und vergessen. Die überwiegende Zahl der abgehörten Telefone sind heute Handys. Die neue Kommunikationswelt hat aber auch neue Überwachungsmöglichkeiten geschaffen, die sich längst nicht mehr nur auf den übermittelten Inhalt beziehen. Scheinbare Randdaten – Verbindungs-, Verkehrs-, Standortdaten

– ermöglichen es schon im Fall der Mobiltelefonie, Kontakt- und Bewegungsprofile von Personen zu erstellen oder gar ihren momentanen Aufenthaltsort zu peilen. Ein Überblick über besuchte Seiten im Internet erlaubt unter Umständen umfangreiche Aussagen über Konsumverhalten oder gar sexuelle Vorlieben. Jedes neue Kommunikationsmittel ist ein potenzielles Überwachungsinstrument.

Eine Entgrenzung der Überwachung findet auch im engeren geografischen Sinne statt. Sowohl die rechtlichen als auch die technischen Standards der Überwachung werden heute in internationalen oder zumindest EU-weiten Gremien diskutiert. Praktisch geht es dabei längst nicht mehr nur um den nachträglichen Austausch von Informationen, die aus einer Abhöraktion gewonnen wurden, sondern in der Tat um den direkten grenzüberschreitenden Zugriff der Polizeien und Geheimdienste – der „gesetzlich ermächtigten Behörden", wie es im Jargon des Rates der EU heißt – auf die neuen Kommunikationsnetze. Für Polizei und Geheimdienste mag sich die in der Werbung versprochene Wunderwelt der Kommunikation als Welt von Cyberkriminellen darstellen. Die NutzerInnen der Netze sollten sich statt dessen um den Schutz ihrer persönlichen und politischen Freiheiten sorgen. Das Ende der Privatsphäre ist dabei allerdings kein Horrorszenario, sondern eine reale Gefahr.

****

Die Versammlungsfreiheit ist das einzige politische Grundrecht, das eine kollektive Einmischung in das politische Geschehen außerhalb der etablierten politischen Formen ermöglicht. Die kommende Ausgabe von Bürgerrechte & Polizei/CILIP wird sich den verschiedensten Formen widmen, in denen BürgerInnen dieses zentrale Grundrecht wahrnehmen. Notgedrungen geht es dabei immer auch um seine politischen und polizeilichen Einschränkungen.

Heiner Busch ist Redakteur von Bürgerrechte & Polizei/CILIP.

Cybercrime

Die Zukunft elektronischer Überwachung

von Albrecht Funk

Die neuen digitalen Informationstechnologien, mit deren Hilfe wir in der virtuellen Realität des Internets kommunizieren und konsumieren, recherchieren und Geschäfte abwickeln, haben ihre Unschuld verloren. Polizei und Geheimdienste wittern hinter der angeblichen Anonymität des Netzes Kriminelle und fordern neue Überwachungsmöglichkeiten.

Nicht mehr die neue Ökonomie der Informationsgesellschaft macht Schlagzeilen, sondern Kriminelle, die bei der Tatbegehung von den Segnungen digitaler Telekommunikation profitieren: Päderasten, die Kinderpornographie in internationalen Usergroups austauschen, Drogenschmuggler, die ihre Geschäfte über Mobiltelefon nur noch verschlüsselt betreiben und dabei die neueste Krypto-Software verwenden – und natürlich Terroristen, die – so die Vermutung von „Experten" – geheime Botschaften in unschuldige Webseiten postierten und so weltweite Netzwerke steuern. Auch die Hacker und Cyberpunks, die in der Vergangenheit die Rolle der Bösewichte, die das Gute fördern, spielten, büßen ihren Robin-Hood-Nimbus ein.

Sicherheitsapparate haben den Missbrauch des Internets durch Kriminelle und die Frage, wie im Cyberspace für Recht und Ordnung gesorgt werden kann, bereits Anfang der 90er Jahre zum Gegenstand von Forderungen nach erweiterten Zuständigkeiten und Eingriffsbefugnissen gemacht. Die Strafverfolgung drohe – so die Klage von FBI und BKA – an den technischen und rechtlichen Hürden der notwendigen elektronischen

Überwachung des Cyberspace durch die Polizei zu scheitern.[1] Die Geheimdienste wiederum, allen voran die US-amerikanische NSA, begannen die neuen Möglichkeiten elektronischer Überwachung extensiv zu nutzen, vor allem im Ausland, wo ihr Informationshunger keine verfassungsrechtlichen Grenzen kennt.[2] Sicherheitsexperten begannen zugleich davor zu warnen, dass die Angriffe von Terroristen, Erpressern und Schurkenstaaten die Sicherheit der für das Funktionieren unserer Gesellschaften bedeutsamen Infrastruktur bedrohten.[3]

Zum Politikum wurde Cybercrime jedoch erst in dem Maße, wie das Internet nicht mehr nur die Angelegenheit einer kleinen Gemeinde von Computerfachleuten war, sondern sich zu einem wirtschaftlich bedeutsamen Raum entwickelte. Sicherheit und Ordnung des Cyberspace wurden zur Vorbedingung für das weitere Wachstum des Internet und der IT-Industrie.[4] Die Gesetzgebungsmaschine, mit deren Hilfe dem gesetzlosen Treiben Einhalt geboten werden soll, gewann Mitte der 90er Jahre rasch an Fahrt. Und da das Internet ein potentiell globales Kommunikationsnetz darstellt, wurde Cybercrime zugleich auf die Agenda internationaler Gremien gesetzt: vom Europarat über die G8 und die OECD bis hin zu öffentlich kaum bekannten Organisationen wie der World Intellectual Property Organization (WIPO) oder dem International Narcotics Control Board (INCB).

Beherrschendes Thema der nationalen und internationalen Expertengremien ist der Kontrollverlust von Polizei und Justiz, die – so die Annahme – mit den vorhandenen Instrumentarien der wachsenden Gesetzlosigkeit im Cyberspace nicht Herr werden können. Die Anonymisierung von Nachrichten ermögliche es häufig nicht, die kriminellen Urheber aufzuspüren. Gesetzliche Beschränkungen der Überwachung digitaler Kommunikation und Datenströme würden die Ermittlungen der Strafverfolgungsbehörden erschweren. Die Grenzenlosigkeit des Internet er-

1 vgl. für die USA: Diffie, W; Landau, S.: Privacy on the line. The Politics of wiretapping and Encryption, Cambridge 1999, pp. 194-195, 207-208; Commission on the advancement of Federal law enforcement: Law Enforcement in a new century and a changing world, Washington 2000, pp. 76-82

2 Bamford, J.: Body of Secrets. Anatomy of the Ultra-Secret National Security Agency, New York 2002; Ders.: The Puzzle Palace, New York 1982

3 National Security Council: Computers at risk, Washington 1991

4 s. Drake, W.J.: The National Information Infrastructure debate: Issues, interests, and the Congressional Process, in: Drake, W.J. (ed.): The New Information Infrastructure, New York 1995, pp. 305-344

laube es transnational organisierten Verbrechern, ihre Tätigkeit vor nationalen Strafverfolgungsbehörden zu verstecken. Frei zugängliche Software ermögliche es Hackern und Crackern, selbst in gut gesicherte Systeme einzudringen und Datenströme anzuzapfen.[5]

Die mitgelieferten Fakten unterstützen die weitreichenden Forderungen der Sicherheitsfachleute nur in den wenigsten Fällen. Hinter den Steigerungsraten von 60-70%, die deutsche und US-amerikanische Kriminalstatistiken jährlich bei der Computerkriminalität registrieren, verbergen sich zunächst und vor allem Verstöße gegen das Urheberrecht oder Computerbetrug – gewöhnliche Eigentumskriminalität unter Zuhilfenahme des Internet, deren Verfolgung nur in den wenigsten Fällen neue Überwachungsbefugnisse erfordert. Es fehlt nach wie vor an systematischen, empirischen Belegen für Antworten auf die Frage, wo wer mit welchen Methoden das bestehende System der Strafverfolgung grundsätzlich in Frage stellt, wie Doris Dennig für die USA und Großbritannien festhielt.[6] Ebenso zutreffend ist diese Aussage für Deutschland, wo das Justizministerium zwar beim Max-Planck-Institut eine Studie zur Abhörpraxis nach altem Recht in Auftrag gegeben hat, zugleich jedoch mit den neuen §§ 100g und h der Strafprozessordnung erst einmal normative Fakten geschaffen hat.[7]

Mutmaßungen über die Ausbreitung des Cybercrime kritisch unter die Lupe zu nehmen, bedeutet nicht, die Augen vor der Wirklichkeit zu verschließen. Die BewohnerInnen des Netzes sind keine besseren BürgerInnen, umso weniger, als die globale Reichweite und der (zumeist illusionäre) Glaube, anonym agieren zu können, abweichendes Verhalten nur weiter befördern. Dass Individuen oder Gruppen den Raum neuer Möglichkeiten vermehrt für unmoralische, verwerfliche Ziele nutzen, ist kaum zu bestreiten. Cybercrime ist wie jede andere Form ungesetzlichen Verhaltens eine soziale Tatsache, wie Emile Durkheim vermerkt. Sie ist

5 Einen guten Überblick bietet Biegel, S.: Beyond our control? Confronting the limits of our legal system in the Age of cyberspace, Cambridge 2001; President's Working group on Unlawful Conduct on the Internet: The Electronic Frontier. The Challenge of unlawful conduct involving the use of the Internet, Washington 2000, http://www.usdoj.gov/criminal/cybercrime/unlawful.htm

6 Denning, D.E.; Baugh, W.E.: Hiding crime in cyberspace, in: Thomas, D.; Loader, B. (eds.): Cybercrime, London, New York 2000, p. 129f.

7 Albrecht, H.J. u.a.: Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b StPO, www.iuscrim.mpg.de/forsch/krim/albrecht/html

eine unvermeidbare Folge der Bemühen staatlicher Autoritäten, die Allgemeingültigkeit gesellschaftlicher Ordnung dadurch zu demonstrieren, dass abweichendes Individualverhalten verfolgt und negativ sanktioniert wird. Versuche der NetzbenutzerInnen, soziale Normen für das Verhalten von Individuen im Internet und virtuellen Gemeinschaften wie Lamda-Moo zu formulieren, gab es früh. Zum Kriminalitätsproblem wurde der Cyberspace jedoch erst in den letzten Jahren, im Zuge der Bemühungen staatlicher Autoritäten, den zum anarchischen und rechtlosen Raum deklarierten Cyberspace zu ordnen und zu regulieren.

Die Formel vom Cybercrime als „Missbrauch" des Internet führt deshalb in die Irre. Sie verschleiert, dass der Ruf nach Kriminalisierung sich nicht von der Frage trennen lässt, wie der neu geschaffene Raum gesellschaftlicher Kommunikation politisch gestaltet und gebraucht werden soll. Hinter den moralischen Kreuzzügen gegen Kinderpornographie und „islamischen Terrorismus", dem Ruf nach Kriminalisierung der Softwarepiraten und der verstärkten elektronischen Überwachung verbergen sich Interessenkoalitionen privater und staatlicher Akteure, die mit aller Macht die zukünftige Ordnung der „public rights" und „public wrongs" im Cyberspace in ihrem Sinne zu gestalten suchen. Die Diskussion um Cybercrime dreht sich nicht um Gesetzlosigkeit und Missbrauch, sondern um die zukünftige Architektur des Raumes öffentlicher und privater Kommunikation im Internet.[8] Bei den transatlantischen Bemühungen, dem Kopieren von Musik, Bildern oder Software mit neuen Strafbestimmungen zu begegnen, geht es nicht primär um den Schutz der Urheberrechte, sondern vor allem um die Aushöhlung der „public domain" mit „open codes" und freien Zugangsmöglichkeiten zugunsten einer kommerziellen Dot.Com-Öffentlichkeit. Neue Strafnormen für die „Störung des Systems", das unerlaubte Eindringen in andere Systeme oder die Datenveränderung kriminalisieren zwar die Aktivitäten von Hackern und Crakkern, bieten jedoch dem individuellen PC-Nutzer oder Systembetreiber kaum zusätzliche Sicherheit. Im Gegenteil: Die Kriminalisierung bedeutet zwangsläufig mehr „policing", mehr elektronische Überwachung – ein Prozess, der wie die „Internationale AG Datenschutz in der Telekommu-

8 Siehe Lessig, L.: Code and other laws of cyberspace, New York 1999

nikation“ befürchtet, „zu einer erheblichen Absenkung des Datenschutzstandards für alle Nutzer von Telekommunikationsnetzen führen kann.“[9]

Der symbolische Gebrauch des Strafrechts wälzt die Risiken und Kosten einer ungesicherten Infrastruktur auf die Endnutzer ab, während die Vertreiber notorisch unsicherer Software in den USA vom Gesetzgeber bewusst vor weitreichenden Schadensersatzklagen geschützt werden. Ansonsten sei der technische Fortschritt und das Wachstum der Branche, der Wirtschaft generell und damit auch der Gesellschaft insgesamt gefährdet. Die Gefahr eines neuen High-Tech-Terrorismus schließlich, der gezielt gegen die Infrastruktur der neuen Informationsgesellschaften gerichtet ist, diente in der Agenda der amerikanischen Regierung für den Ausbau der National Information Infrastructure schon 1994 dazu, die Sicherung der kritischen Systeme zum Gegenstand nationaler Sicherheitspolitik zu erheben und damit zum Objekt geheimdienstlicher und militärischer Einflussnahme. Mit dem, was als Cyberterrorismus antizipiert wird, haben die Terrorakte des 11. September zwar wenig zu tun, trotz aller (Des-)Informationen über die technische Omnipotenz bin Ladens. Den Forderungen nach einer stärkeren (elektronischen) Überwachung und Sicherung des Cyberspace haben die Terrorakte jedoch neuen Auftrieb gegeben.

Als empirische Beschreibung einer bestimmten Verbrechenswirklichkeit bleibt die Diskussion um Cybercrime, -terrorismus und -warfare dürftig. Beherrscht wird sie von der interessierten Antizipation drohender Übel, welche die anvisierte Sicherheitsarchitektur des Cyberspace legitimiert. Materielle Gestalt gewinnt Cybercrime nicht dort, wo Gefahren beschworen werden, sondern dort, wo die zur Abwehr dieser Gefahren erforderliche elektronische Überwachung normiert wird.

Cyberspace als elektronischer Überwachungsraum

Visionäre wie der frühere Präsident des Bundeskriminalamts Horst Herold haben früh erkannt, dass Datenverarbeitung und computergestützte Kommunikationstechnologien Strafverfolgungsbehörden und Geheimdiensten bislang unbekannte Möglichkeiten der Überwachung eröffnen.

9 Gemeinsamer Standpunkt zu Datenschutzaspekten des Entwurfs einer Konvention zur Datennetzkriminalität des Europarates, 28. Sitzung der Internationalen AG Datenschutz in der Telekommunikation, in: Berliner Beauftragter für Datenschutz und Akteneinsicht (Hg.): Dokumente des Datenschutzes, Berlin 2000, S. 71

Heute erlauben die Digitalisierung und Bündelung aller möglichen Formen der Telekommunikation, die Überwachung und Kontrolle von Datenströmen in einem Maße auszudehnen, das vor 30 Jahren undenkbar war. Technisch lässt sich durch die Erfassung der Daten, die BürgerInnen bei der Nutzung ihrer Mobiltelefone und Kreditkarten, ihrer Computer und Webbrowser hinterlassen, das Netzwerk ihrer sozialen Kommunikation weitgehend rekonstruieren, ohne dass auch nur der geringste Versuch unternommen wird, den Inhalt der Kommunikation selbst zu überwachen. Programme wie Carnivore ermöglichen es, aus Datenpaketen, die für die überwachende Behörde relevanten Informationen herauszufiltern oder durch die gezielte Infiltrierung von Computern (durch „legale", staatlich genutzte Trojan Horse-Progamme wie DIRT oder Magic Lantern) den gesamten Datenverkehr einer Person zu überwachen.[10] Technisch wird der Cyberspace zu einem potentiell schrankenlosen Überwachungsraum, in dem die physische Separierung von Privaträumen und öffentlichen Räumen ebenso hinfällig wird wie die Trennung zwischen Form und Inhalt von Kommunikation.

Was technisch möglich ist – nämlich die Konstruktion des Cyberspace als sicherheitspolizeilichem Raum totaler elektronischer Überwachung – verstößt jedoch gegen Grundprinzipien einer freiheitlichen und demokratischen Organisation von Staat und Gesellschaft. DatenschützerInnen und die neuen Bürgerrechtsorganisationen der Netizens (NetzbürgerInnen) beharren deshalb auf einer Architektur des Cyberspace, die auf drei verfassungsrechtlichen Pfeilern beruht: auf der strikten rechtsstaatlichen Begrenzung staatlicher Eingriffe in die Rechte der BürgerInnen, auf einer weder staatlich noch durch private Monopole kontrollierten, demokratischen Öffentlichkeit und auf dem Schutz privater Kommunikation durch einen transparenten, das Recht auf informationelle Selbstbestimmung achtenden Datenschutz.

Die kritischen Einwände und Proteste von ExpertInnen und Bürgerrechtsgruppen haben die rapide Transformation des Cyberspace in einen elektronischen Überwachungsraum nicht aufhalten können. An der von Sicherheitsapparaten wie Regierungen seit der Entstehung moderner Staaten vertretenen Position, dass es keinen Bereich menschlicher Kommunikation geben darf, der dem Zugriff von Polizei und Geheimdiensten

10 s.: How Carnivore works, www.howstuffworks.com/carnivore.htm

prinzipiell entzogen sein kann, rütteln nur wenige.[11] Strittig ist in der gesetzgeberischen Diskussion deshalb nicht, dass die neuen digitalen Telekommunikationsnetze der elektronischen Überwachung durch Sicherheitsapparate zugänglich sein müssen. Die Frage dreht sich vielmehr nur darum, wie, in welchen Fällen, in welchem Umfange, mit welchen rechtsstaatlichen Kontrollen dies geschehen soll.

Die Entscheidung, den Cyberspace durch vorgeschriebene Schnittstellen und „digital switches" überwachbar zu machen, geht einher mit einer massiven Ausweitung der Möglichkeiten von Nachrichtendiensten und Polizeien, Datenströme zu überwachen, zu filtern und zu speichern. Dies gilt für die USA wie für die BRD, trotz aller Beteuerungen (so auch der rot-grünen Bundesregierung im Falle der Telekommunikationsüberwachungsverordnung, TKÜV), dass von einer „Ausweitung" der polizeilichen und geheimdienstlichen Überwachungsbefugnisse und -voraussetzungen keine Rede sein könne. Die Eingriffsvoraussetzungen für intensive Einzelüberwachungen, deren Kosten in den USA mit durchschnittlich 50.000 Dollar angesetzt werden, und das Abhören oder Mitlesen von Kommunikationsinhalten sind in der Tat – zumindest vor dem 11.9. – kaum verändert worden.[12] Die Revolution vollzieht sich hinter der Fassade der alten Befugnisse, mit denen Telefongespräche abgehört, Briefe geöffnet und selbst intime Tagebucheintragungen strafprozessual verwertet werden dürfen. Was die amerikanischen Pen/Trap und Wiretap Statutes, die Novellierung des G10-Gesetzes, das Telekommunikationsgesetz (TKG) und die TKÜV verbindet, ist das Bemühen der Gesetzgeber, die Datenströme digitaler Kommunikation durch drei Maßnahmebündel umfassend und extensiv zugänglich zu machen.[13]

Das erste zielt auf die Durchsetzung einer abhörfreundlichen Architektur digitaler Netze bei den privaten Betreibern. So schreibt der amerikanische Communications Assistance Law Enforcement Act (CALEA), abgestuft nach der Intensität der Netznutzung, sowohl die bereitzustel-

11 die gut begründete Gegenposition findet sich bei: Diffie; Landau a.a.O. (Fn. 1)

12 zusammenfassend zum US-Wiretapping Report 2000, www.cdt.org/wiretap/wiretap_overview.html. Die nicht direkt vergleichbaren Angaben für Abhörmaßnahmen im Bereich der Strafverfolgung nach Title III (Abhören der Kommnunikation) liegen mit ca. 1200 niedrig im Vergleich zur Bundesrepublik.

13 s. für die USA: US Department of Justice: Seizing Computers and Obtaining Evidence in Criminal Investigation, www.cybercrime.gov/searchmanual.htm#I und www.cdt.org/wiretap/wiretap_overview.html

lenden Kapazitäten für simultan nutzbare Überwachungen (zwischen 48.000 und 52.000) als auch die Form des Zugriffs vor (kontinuierlich, online).[14]

Das zweite Bündel gesetzgeberischer Maßnahmen sichert den Zugriff der Sicherheitsbehörden auf die in der digitalisierten Telekommunikation in Hülle und Fülle anfallenden Daten rechtlich ab: angefangen von den Kundenkarteien bis hin zu Listen aller Anrufe/E-Mails etc. für eine bestimmte Adresse oder der Liste aller Aktivitäten eines bestimmten Telnehmers (Bestands- und Verkehrsdaten bzw. pen register bzw. track/trace). Die Unterscheidung zwischen einer bloßen Erfassung der Anrufe von einem und für einen Anschluss und dem eigentlichen Abhören, die im 20. Jahrhundert Überwachung begrenzte, verschwimmt in der digitalisierten Telekommunikation. Die alte Unterscheidung wird zum Einfallstor für die extensive Erhebung einer Vielzahl digitaler Daten, indem die Erhebung rechtlich als ein, verglichen mit der Überwachung von Kommunikationsinhalten, geringerer Eingriff interpretiert wird. Faktisch ist jedoch in vielen Bereichen (Webnutzung, Standortbestimmung von Mobiltelefonnutzern etc.) die Erfassung dieser „Verkehrsdaten" von einem Erfassen der Inhalte nicht zu trennen. Sie erlauben die Erstellung von Datenprofilen, deren Tiefe und inhaltliche Aussagekraft in vielen Fällen weit über das hinausgehen, was einE BürgerIn beim Abhören seiner/ihrer Gespräche hinzunehmen hat.

Ein drittes Maßnahmebündel schließlich erzwingt von den privaten BetreiberInnen, Daten für polizeiliche und geheimdienstliche Zwecke vorrätig zu halten – und zwar auch über den Zeitpunkt hinaus, wo dies aus betrieblichen Gründen erforderlich ist (siehe etwa die Heraufsetzung der Speicherfristen für Verbindungsdaten in der Telekommunikations-Datenschutzverordnung, TDSV).

Cyberspace: (nicht) überwachbarer Überwachungsraum?

Der extensive Zugriff auf eine Flut digitalisierter Daten hat die Möglichkeiten der Sicherheitsapparate, Bewegungsprofile zu erstellen, Datamining oder Rasterfahndungen zu betreiben, erheblich verstärkt. Die Effektivität solcher Methoden hängt jedoch maßgeblich davon ab, inwieweit auch der Inhalt der von Verdachtspersonen oder potentiellen Infor-

14 Diffie; Landau a.a.O. (Fn. 1), p. 198 und www.AskCALEA.net

mationsquellen generierten Datenströme abgehört oder gelesen werden kann. Die Frage, die Geheimdienste wie Polizeien gleichermaßen beunruhigt, ist aber gerade, ob die staatlichen Sicherheitsapparate die Segnungen der Digitalisierung von Informationen genießen können, ohne zugleich dem Alptraum nicht mehr dechiffrierbarer und damit überwachbarer digitaler Datenströme ausgesetzt zu sein. Das Konzept von zwei getrennten „Public Keys" für Chiffrierung und Dechiffrierung revolutionierte Mitte der 70er Jahre eine bis dahin im Arkanbereich der Geheimdienste betriebene Kryptografie. Da diese Methode prinzipiell jeder Privatperson die Möglichkeit einräumt, ihre Daten vor jedem fremden Zugriff zu schützen, wurde die Public Key-Kryptologie von den Geheimdiensten sofort als massive Bedrohung ihres Monopols wahrgenommen.[15] Zunächst bemühte sich die US-Regierung schlicht, die Verbreitung der Methode zu verhindern. Dann suchte sie die amerikanische Vorherrschaft im IT-Sektor dazu zu nutzen, den Export von Krypto-Software mit mehr als 64 Bits zu verbieten, die Anfang der 90er Jahre nur schwer oder nicht zu dechiffrieren waren. Zugleich bot sie national wie international einen „Escrowed Encryption Standard" an, d.h. einen geheimen, alleine den US-Sicherheitsbehörden bekannten Algorithmus, der als Verschlüsselung in einen nicht manipulierbaren Chip (Clipper) inkorporiert wird. Der Clipper-Versuch scheiterte am Desinteresse ausländischer Staaten, die sich nicht in die kryptografische Obhut der USA begeben wollten, – aber auch am Widerstand amerikanischer Computerexperten. Auch das Exportverbot erwies sich als Bumerang, indem es ausländischen Anbietern (wie Brokate aus der BRD) auf dem Feld starker Verschlüsselung Wettbewerbsvorteile verschaffte.

Faktisch handelt es sich bei der Frage, wie stark die Kryptografie für die Bürger im Netz sein darf, immer noch um ein theoretisches Problem. Selbst in den USA wird im Wiretap-Bericht des Jahres 2000 die Zahl der Fälle, in denen Strafverfolgungsbehörden den Inhalt überwachter Kommunikation nicht entschlüsseln konnten, mit Null angegeben.[16] Doch in dem Maße, wie die Netizens konkret erfahren, wie ungeschützt ihre private Kommunikation im Internet ist, wird auch deren Nachfrage nach

15 Diffie; Landau a.a.O. (Fn.1), pp. 35-38 u. 60-63. Diffie war einer der Erfinder der Public Key Methode.

16 Wiretap Report 2000, www.uscourts.gov/wiretap00/2000wttxt.pdf, p. 11

Public Key-Verschlüsselungsprogrammen wachsen, die in einer für Laien handhabbaren Form angeboten werden.

Das FBI experimentiert deshalb bereits mit Trojan Horse-Programmen (Magic Lantern), die es ihm erlauben, Passwort und Algorithmus beim Nutzer selbst abzufragen. Und es mehren sich die Meldungen, dass die amerikanische Regierung durch Kooperation mit und Druck auf die Anbieter von Kryptoprogrammen (wie Pretty Good Privacy) und Anti-Virus Software (wie McAfee) die Unsichtbarkeit ihrer Überwachung sicherzustellen sucht.[17]

Mit dem Kampf gegen das Verbrechen hat der technologische Wettkampf zwischen verfeinerter elektronischer Überwachung und Kryptografie wenig zu tun. Verschlüsselung spielt nicht nur hier und heute keine Rolle für die Bekämpfung von Cybercrime. Auch in der Zukunft wird die Existenz starker Kryptoprogramme, wie Duffie/Landau plausibel begründen, nur von untergeordneter Bedeutung für Zwecke der Strafverfolgung sein.[18]

Der Streit um die Kryptografie ist nur verständlich als Kampf um Vorherrschaft im Cyberspace. Mit ihrem Clipper Chip diente sich die amerikanische Regierung als vertrauensvoller Wahrer der Sicherheit des Cyberspace und damit aller Netizen an – im Austausch für die Möglichkeit, als Verwahrer des Schlüssels Daten dort lesen und abhören zu können, wo ihr dies aus Gründen der (nationalen) Sicherheit erforderlich erscheint. Der erste Versuch eines Staates, sich als „trustfull third party“ zu etablieren, scheiterte. Weitere Versuche werden folgen, durch die USA, die EU und andere lokale Leviathane. Wer über den Code verfügt, übt Herrschaft aus im Cyerspace, national und international. Wer keine Schlüssel hat, büßt Macht ein.

Albrecht Funk ist Mitherausgeber von Bürgerrechte & Polizei/CILIP und lebt derzeit in Pittsburgh (USA).

17 McCullagh, D.: Lantern Door Flap ranges at, www.wired.com/news/print/0,1294, 48648,00.html

18 Diffie; Landau a.a.O., pp. 225-245

Telekommunikationsüberwachung

Wer darf wann was. Eine Kurzübersicht

von Norbert Pütter

Das Recht der Telekommunikationsüberwachung ist unübersichtlich. Die Regelungen sind auf verschiedene Gesetze und Verordnungen verstreut; die ausufernde Gesetzessprache versteckt die Ausweitung der Überwachung häufig hinter Querverweisen und Schein-Konkretisierungen; und vermehrt treten Ort und Umstände der Kommunikation in das Zentrum der Überwachung. Im Folgenden können nur einige Grundzüge aus diesem Geflecht aufgezählt werden.

Die gesetzlichen Bestimmungen unterscheiden sich nach den Behörden, die die Telekommunikation (TK) überwachen dürfen. Das sind in Deutschland die Polizei, der Zoll und die drei Geheimdienste. In den jeweiligen Gesetzen wird zudem unterschieden zwischen der Überwachung der Kommunikationsinhalte und der Überwachung der sonstigen Daten, die bei der TK anfallen. Außerdem dient die TK zunehmend als Mittel der Ortung von Personen und der Identifizierung von TK-Anschlüssen.

TK-Überwachung durch die Polizei

Die zentralen Vorschriften für die polizeiliche Überwachung der TK sind die §§ 100a der Strafprozessordnung (StPO). Sie erlauben die „Überwachung und Aufzeichnung der Telekommunikation“, wenn bestimmte Tatsachen den Verdacht begründen, dass eine Person eine der katalogartig aufgelisteten Straftaten begangen hat oder an ihnen beteiligt war. Nach dem „Telekommunikationsgesetz“ ist unter TK das Aussenden, Übermitteln und Empfangen von Nachrichten jeglicher Art in der Form

von Zeichen, Sprache, Bildern oder Tönen mittels elektromagnetischer oder optischer Signale zu verstehen.
Der Vortatenkatalog des § 100a ist in den letzten Jahrzehnten ständig erweitert worden. Ursprünglich lag sein Schwerpunkt im Bereich des Staatsschutzes, mittlerweile sind aber eine Vielzahl neuer Katalogtaten hinzugefügt worden. Kaum eine StPO-Novelle der letzen Jahre hat auf eine Ausweitung von § 100a verzichtet. Sein genauer Umfang ist nur schwer zu erfassen, da etwa durch die §§ 129, 129a Strafgesetzbuch (kriminelle oder terroristische Vereinigung) oder die Geldwäsche als Katalogtat erhebliche Ausweitungen auf andere „Vortaten" möglich sind.

Die Überwachung muss von einem Gericht schriftlich angeordnet werden. Bei Gefahr im Verzuge kann die Staatsanwaltschaft die Maßnahme für die Dauer von maximal drei Tagen anordnen. Die Anordnung darf sich gegen den Beschuldigten richten oder gegen Personen, von denen angenommen wird, dass sie Informationen für den Beschuldigten weitergeben oder entgegennehmen. Unabhängig vom Grund der Überwachung dürfen die Erkenntnisse aus der TK-Überwachung zur Aufklärung aller Katalogtaten des § 100a genutzt werden.

Seit 1.1.2002 ist der Zugriff der Ermittlungsbehörden auf die „TK-Verbindungsdaten" neu geregelt. Diese Daten umfassen u.a. die Standortkennung, die Rufnummern des anrufenden und angerufenen Anschlusses, Beginn und Ende der Verbindung und die in Anspruch genommenen TK-Dienstleistungen. Diese Art der Überwachung ist nicht an den Katalog des § 100a gebunden, sondern an den Verdacht auf eine „Straftat von erheblicher Bedeutung" – ein rechtlich unbestimmter Begriff. Die Anordnung auf Preisgabe der TK-Verbindungsdaten ist nicht auf eine bestimmte Person und dessen Anschluss begrenzt, sondern es „genügt eine räumlich und zeitlich hinreichend bestimmte Bezeichnung der TK, über die Auskunft erteilt werden soll" (§ 100h StPO).

Der polizeiliche Einsatz des sogenannten IMSI-Catchers zur Ermittlung von Standort, Geräte- und Kartennummer von Mobiltelefonen geschieht auf der Grundlage von § 100c StPO, der „besondere für Observationszwecke bestimmte Mittel" bei Ermittlungen wegen einer „Straftat von erheblicher Bedeutung" erlaubt. (S. hierzu den Beitrag von Björn Gercke in diesem Heft.)

TK-Überwachung durch das Zollkriminalamt

Seit 1992 ist das Zollkriminalamt zur Überwachung der TK ermächtigt. Das Ziel der Überwachung ist „die Verhütung von Straftaten nach dem Außenwirtschaftsgesetz oder dem Kriegswaffenkontrollgesetz“. Die von einem Landgericht (bei Gefahr im Verzug vom Bundesminister der Finanzen) zu erlassende Überwachungsanordnung kann verdächtige Personen, deren Kontaktpersonen oder das Unternehmen betreffen, in dem diese Personen arbeiten. Neben der Beschränkung auf Delikte aus den beiden genannten Gesetzen unterscheidet sich die TK-Überwachung des Zolls von der der Polizei durch ihre präventive Zielsetzung: Da es um die Verhinderung zukünftiger Taten geht, werden die Anschlüsse von Personen und Firmen überwacht, von denen angenommen wird, dass sie jene Taten *planen*.

TK-Überwachung durch die Geheimdienste

Die TK-Überwachung der Geheimdienste ist im „G 10-Gesetz“ geregelt, das im letzten Jahr novelliert wurde. Die 17 deutschen Verfassungsschutzämter (VfS), der Militärische Abschirmdienst (MAD) und der Bundesnachrichtendienst (BND) werden mit diesem Gesetz zur TK-Überwachung und -Aufzeichnung ermächtigt. Die Überwachung ist an einen Katalog von Straftaten gebunden, der neben den klassischen Staatsschutzdelikten wie Hochverrat, Landesverrat oder die Gefährdung des demokratischen Rechtsstaates auch andere Delikte enthält – etwa § 129a StGB (terroristische Vereinigung) oder eine Reihe „normaler Straftaten“, sofern sie sich gegen die „freiheitliche demokratische Grundordnung“ richten. Voraussetzung für die Überwachung ist der Verdacht, dass jemand diese Taten „plant, begeht oder begangen hat“. Die Anordnung zur Überwachung, die sich auch auf zukünftige TK erstrecken kann, erfolgt durch die Behörden. Für die Maßnahmen vom MAD, BND und Bundesamt für VfS ist (außer bei Gefahr im Verzug) die vorherige Zustimmung der G 10-Kommission des Bundestages erforderlich. Sofern die Erkenntnisse aus der Überwachung dazu beitragen, dass eine der Katalogtaten verhindert, verfolgt oder aufgeklärt werden kann, können diese an die Strafverfolgungsbehörden weitergegeben werden.

Eine Sonderstellung nimmt die „strategische“ TK-Überwachung durch den BND ein. Diese ist nicht auf einzelne Anschlüsse begrenzt, sondern umfasst die „internationalen Telekommunikationsbeziehungen“. Der Festlegung, welche TK-Beziehungen durch den BND überwacht werden, muss das Parlamentarische Kontrollgremium des Bundestages zu-

stimmen. Die Überwachung ist zulässig, um bestimmte Gefahren rechtzeitig erkennen und ihr begegnen zu können. Zu den im Gesetz genannten Gefahren gehört u.a. ein bewaffneter Angriff auf die Bundesrepublik, die unerlaubte Verbreitung von Kriegswaffen oder Technologien, der Rauschgiftimport in größerem Ausmaß oder die internationale Geldwäsche „in Fällen von erheblicher Bedeutung". Bei seiner strategischen Überwachung darf der BND nur Suchbegriffe verwenden, die einen unmittelbaren Bezug zu jenen Gefahrenbereichen erkennen lassen. Die Weitergabe der BND-Erkenntnisse aus der strategischen Überwachung ist an die anderen Geheimdienste, an das Bundesamt für Wirtschaft und Ausfuhrkontrolle und „an die mit polizeilichen Aufgaben betrauten Behörden" zulässig – jeweils gebunden an bestimmte Gefahren oder den Verdacht auf bestimmte Straftaten.

Durch das „Terrorismusbekämpfungsgesetz" haben die drei Dienste seit Januar 2002 auch Zugang zu den „TK-Verbindungsdaten" und den Teledienstnutzungsdaten, d.h. Kartennummer, Standort, Anschlussnummern, Beginn und Ende der Verbindungen, in Anspruch genommene Dienstleistungen etc. Auch dem Antrag auf diese Auskünfte muss die G 10-Kommission vorab zustimmen. Ebenfalls seit dem 1.1.2002 darf das Bundesamt für VfS den „IMSI-Catcher" zur Ortung und Überwachung von Mobiltelefonen einsetzen.

Technisch-praktische Umsetzung

Durch die „TK-Überwachungsverordnung" vom 22.1.2002 sind die Standards festgeschrieben worden, die die Betreiber von TK-Anlagen erfüllen müssen, um die Überwachungen durch Polizei, Zoll und Geheimdienste zu gewährleisten. (Die TKÜV gilt nicht für die „strategische Überwachung" des BND.) U.a. werden die Betreiber verpflichtet, den Sicherheitsbehörden „eine vollständige Kopie der Telekommunikation bereitzustellen", sie müssen dafür Sorge tragen, dass die Überwachung „unverzüglich" erfolgen kann und geheim bleibt, und sie müssen gewährleisten, dass mehrere Behörden denselben Anschluss gleichzeitig überwachen können. Die Liste der von den Anbietern bereitzustellenden Daten ist umfangreich; sie reicht von den Rufnummern, die von einem überwachten Anschluss angerufen werden oder diesen anrufen oder versuchen anzurufen, über Zeiten und Dauer der TK(-Versuche) bis zu den in Anspruch genommenen TK-Diensten, deren Merkmale und Kenngrößen bis zum Standort von Mobilanschlüssen (§ 7 TKÜV).

Norbert Pütter ist Redakteur von Bürgerrechte & Polizei/CILIP.

Überwachung des Mobilfunkverkehrs

Das Handy als „Allroundmittel“ zur Ausforschung

von Björn Gercke

Letztes Jahr nutzten in Deutschland bereits rund 50 Millionen Menschen ein Mobilfunkgerät. Den wenigsten dürfte bewusst sein, dass sie den Ermittlungsbehörden damit Möglichkeiten der Überwachung eröffnen, die weit über das klassische Abhören hinausgehen. Die Rechtsprechung nimmt diese Unterschiede kaum zur Kenntnis. Sie hat die neuen Formen der Überwachung weitgehend abgesegnet.

Hinsichtlich der Anzahl der jährlichen Telefonüberwachungen (TÜ) nimmt die Bundesrepublik Deutschland unter den westlichen Staaten seit Jahren einen unrühmlichen Spitzenplatz ein. So haben Böttger/Pfeiffer für den Zeitraum von 1987 bis 1992 aufgezeigt, dass das Risiko, in Deutschland abgehört zu werden, rund dreizehnmal höher war als in den USA, obwohl diese zum gleichen Zeitraum eine erheblich höhere Kriminalitätsrate hatten.[1]

Im Gegensatz zu früheren Erklärungen räumen die Ermittlungsbehörden seit 1995 ein, dass auch die digitalen Funknetze abhörbar sind.[2] Entsprechend der gestiegenen Bedeutung der mobilen Kommunikation kommt der Überwachung von Mobilfunkanschlüssen mittlerweile die tragende Rolle im Rahmen der TÜ zu. Sowohl der Gesetzgeber als auch – fast einhellig – Rechtsprechung und Lehre subsumieren die akustische Überwachung des Mobilfunkverkehrs unproblematisch unter die Er-

1 Böttger, A.; Pfeiffer, Ch.: Der Lauschangriff in den USA und in Deutschland, in: Zeitschrift für Rechtspolitik 1994, H. 1, S. 7-17 (8)

2 Artkämper, H.: Ermittlungsmaßnahmen in Funktelefonnetzen, in: Kriminalistik 1998, H. 3, S. 202-207

mächtigungsgrundlage des § 100a der Strafprozessordnung (StPO), der ursprünglich für den herkömmlichen Festnetzverkehr konzipiert wurde. Der Mobilfunkverkehr, so lautet das simple Argument, weise „lediglich technische Besonderheiten“ auf.[3]

Nur wenige Autoren lassen sich auf die Unterschiede von alter und neuer Technik ein und halten dieser Position entgegen, dass § 100a StPO lediglich die Überwachung genau festgelegter Anschlüsse zulasse. In der Mobilfunktechnik existieren aber gerade keine Anschlüsse, sondern Funkzellen, die jeweils zugleich von mehreren MobilfunkteilnehmerInnen genutzt werden. Deren Geräte schalten sich automatisch in eine Funkstrecke ein, die gerade frei ist. Wenn die Gespräche einer bestimmten Person abgehört werden sollen, wird daher nach den in Betracht kommenden Funkstrecken gesucht, so dass man quasi von einer „Abhörrasterfahndung“ sprechen muss, deren Anwendbarkeit nicht von der Individualkontrolle des § 100a StPO gedeckt ist.[4]

Speicherung und Auswertung der Verbindungsdaten

Bei der digitalen Übertragung fallen aber über das gesprochene Wort hinaus eine Vielzahl von Daten an, die aus Sicht der Strafverfolgungsorgane „kriminalistisch und fahndungstechnisch höchst interessant“ sein sollen.[5] So wird nach Beendigung jedes Gesprächs der sog. Verbindungsdatensatz gespeichert. Dieser muss nach § 7 Abs. 3 Telekommunikations-Datenschutzverordnung (TDSV) erst sechs Monate nach Beendigung der Verbindung gelöscht werden. Er beinhaltet u.a. Datum, Uhrzeit und Dauer des Gesprächs, die Rufnummern der beteiligten Anschlüsse sowie die Standortdaten des Mobilfunknutzers anhand der Funkzellenbestimmung (§ 6 Abs. 1 TDSV). Die Strafverfolgungsbehörden können auf Grundlage des neuen § 100g StPO von den Telekommunikationsanbietern die Herausgabe dieser Verbindungsdaten verlangen.

---

3 ebd., S. 202; zur Gesetzgebung siehe BT-Drs. 13/1139, zur Rechtsprechung vgl. nur: BGH-Ermittlungsrichter, in: Computer und Recht 1998, H. 12, S. 738-741 (739); Nack, A., in: Pfeiffer, G. (Hg.): Karlsruher Kommentar zur Strafprozessordnung, 4. Auflage, München 1999, § 100a, Rn. 6

4 Perschke, St.: Die Zulässigkeit nicht spezialgesetzlich geregelter Ermittlungsmethoden im Strafverfahren, Köln 1997, S.17; ebenso: Riegel, R.: Zur Suche nach Rechtsgrundlagen für die Fernmeldeaufklärung oder strategische Rasterfahndung durch den Bundesnachrichtendienst, in: Zeitschrift für Rechtspolitik 1993, H. 12, S. 468-471 (470 f.)

5 Artkämper a.a.O. (Fn. 2), S. 204

Lokalisierung und Bewegungsbilder im Stand-by-Betrieb

Von besonderem Interesse für die Strafverfolgungsorgane sind jedoch die Standortdaten, die auch im bloßen Stand-by-Betrieb anfallen, also ohne dass ein Gespräch tatsächlich geführt oder auch nur gewählt wurde. Diese werden technisch zwingend permanent festgestellt, um die Erreichbarkeit jedes Teilnehmers zu gewährleisten.[6] Je nach Größe der Funkzelle lässt sich der Mobilfunk-Nutzer somit bis auf 30 Meter genau orten.[7]

Durch die Auswertung der Standortdaten lässt sich ein Bewegungsbild des Mobilfunkgerätes im Stand-by-Betrieb gewinnen, das zwar je nach Größe der Funkzelle unterschiedlich detailliert ist, jedoch aufgrund der hohen Frequenz der einzelnen Lokalisierungen nahezu lückenlos ist. Während Verbindungsdaten nur dann anfallen, wenn tatsächlich telefoniert oder TeilnehmerInnen zumindest angewählt wurden, werden die Standortdaten etwa in den D-Netzen alle 2,4 Sekunden festgestellt. Das Mobilfunkgerät mutiert, so der Brandenburgische Datenschutzbeauftragte Alexander Dix, zu einem „stets aktiven Peilsender".[8]

Der Ermittlungsrichter beim Bundesgerichtshof (BGH) hat in einem Beschluss vom 21.2.2001 die Ermittlung der Standortdaten im Stand-by-Betrieb unter § 100a StPO subsumiert.[9] Damit befindet er sich im Einklang mit der überwiegenden Ansicht in der Literatur sowie einer Reihe bereits ergangener unterinstanzlicher Entscheidungen.[10] Eine überzeugende Begründung, weswegen die permanente Feststellung der Position eines Mobilfunkgerätes rechtmäßig sein und wieso sie überhaupt etwas mit (Tele-)Kommunikation zu tun haben soll, bleibt der BGH-Ermittlungsrichter schuldig.

Das Telekommunikationsgesetz (TKG), die TDSV oder die jüngst verabschiedete Telekommunikationsüberwachungsverordnung (TKÜV) kön-

6 Zum genauen technischen Ablauf vgl.: Gercke, B.: Bewegungsprofile anhand von Mobilfunkdaten im Strafverfahren – zugleich ein Beitrag zur Kumulation heimlicher Observationsmittel im Strafverfahren, Kap. 1 B., m.w.N. (erscheint demnächst)

7 Fatah, K.: Spion am Ohr, in: com!online 2001, Nr. 6, S. 132-134 (134); innerhalb der Funkzelle ist durch weitergehende, allerdings aufwendigere Peilmaßnahmen prinzipiell eine noch genauere Ortung des Mobilfunkgerätes möglich, vgl. Landgericht (LG) Berlin, in: Datenschutz und Datensicherheit 1998, H. 12, S. 725 f.

8 Dix, A.: Aktiver Peilsender, in: com!online 2001, Nr. 6, S. 135

9 BGH Ermittlungsrichter, in: Strafverteidiger 2001, H. 4, S. 214-216

10 siehe z.B. Nack a.a.O. (Fn. 3), Rn. 13, sowie LG Aachen, in: Strafverteidiger 1999, H. 11, S. 590f.; LG Dortmund, in: Neue Zeitschrift für Strafrecht 1998, H. 11, S. 577f.; LG Ravensburg, in: Neue Zeitschrift für Strafrecht – Rechtsprechungs-Report 1999, H. 3, S. 84f.

nen insoweit allenfalls bloße Orientierungshilfen sein. Ihre Adressaten sind nicht die Beschuldigten, sondern die Telekommunikationsanbieter. Sie regeln auch nicht die Überwachung, sondern fordern von der Wirtschaft, die technischen Voraussetzungen für die Überwachung bereitzustellen.[11] Eine Ermächtigung für die permanente Feststellung des Standortes müsste sich – wenn schon – aus der Strafprozessordnung selbst ergeben.

Um deren Fehlen auszugleichen, vollführt der BGH ein unzulässiges Ausweichmanöver: Wie zuvor schon das Landgericht Aachen, greift er auf das Fernmeldegeheimnis aus Art. 10 Grundgesetz (GG) zurück.[12] Dieses Grundrecht schützt anerkanntermaßen nicht nur den übermittelten Kommunikationsinhalt, sondern auch die näheren Umstände der (Tele-)Kommunikation.[13] Weil das Grundrecht damit auch die Standortdaten der Kommunizierenden schützt, könne sich der auf § 100a StPO gestützte Eingriff in das Grundrecht automatisch auch auf die Feststellung dieser Daten beziehen. Das würde nichts anderes bedeuten, als dass alle Überwachungsmöglichkeiten, die sich als technische Begleiterscheinungen aus der Telekommunikation ergeben, auch rechtlich machbar wären, sobald nur eine richterliche Anordnung nach § 100a StPO vorliegt.

Der BGH verkennt in eklatanter Weise das Verhältnis von Grundrecht und strafprozessualer Ermächtigungsgrundlage. Funktion des ersteren ist es, Rechtspositionen des Einzelnen zu schützen. Der Eingriff in diese Rechtspositionen ist nur möglich, soweit er sich aus der strafprozessualen Ermächtigungsgrundlage selbst ergibt. Von dem Schutzbereich eines Grundrechtes darf nicht auf den Anwendungsbereich einer strafprozessualen Ermächtigungsgrundlage geschlossen werden, da dies letztlich den Grundrechtsschutz ad absurdum führen würde.[14]

Das Ausweichmanöver des BGH dürfte sich daraus erklären, dass eine eigenständige strafprozessuale Auslegung des Begriffes „Telekommunikation“ keineswegs eine Subsumtion der Positionsfeststellung im Stand-by-Betrieb unter § 100a StPO zulässt. Schon vom Wortlaut her lässt sich die Ortung wohl kaum als Akt der „Kommunikation“ bezeich-

11 vgl. mit ausführlicher Begründung: Gercke a.a.O. (Fn. 6), Kap. IV B. III

12 LG Aachen a.a.O. (Fn. 10), S. 590

13 Bundesverfassungsgericht, Entscheidungen (BVerfGE), Bd. 67, S. 157-185 (172); Bd. 85, S. 386-405 (396)

14 Bernsmann, K.; Jansen, K.: Anmerkung zu LG Aachen, in: Strafverteidiger 1999, H. 11, S. 591-593

nen; es handelt sich vielmehr um eine technisch zwingend-notwendige Voraussetzung für die ständige Empfangsbereitschaft des Mobilfunkgerätes. Wollte man aber tatsächlich jede technische Voraussetzung dem Kommunikationsbegriff zuordnen, drohte dieser so auszuufern, dass letztlich eine völlige Begriffsleere vorliegen würde.[15]

Schließlich verbietet es sich schon angesichts der prinzipiell hohen Eingriffsintensität heimlicher Ermittlungsmethoden, bereits bestehende Ermächtigungsgrundlagen extensiv auszulegen – ein Grundsatz, dem die Rechtsprechung nur noch bedingt nachkommt. Der BGH-Ermittlungsrichter greift nun ein weiteres Mal tief in die juristische Trickkiste: die Standortdatenerfassung weise gegenüber der Überwachung des gesprochenen Wortes eine „bedeutend geringere" Eingriffsintensität auf.[16] Angesichts der verhältnismäßig engen Zulässigkeitsvoraussetzungen für eine Anordnung nach § 100a StPO könnte eine solche Argumentation auf den ersten Blick noch als besonders „grundrechtsfreundlich" erscheinen. Erstens aber handelt es sich bei § 100a StPO um eine abschließende Regelung, die als solche schon prinzipiell keine – vermeintlich – „milderen" Eingriffe („Minus-Maßnahmen") zulässt.[17] Zweitens ist die Standortdatenerfassung eben kein milderes Mittel, sondern etwas völlig anderes. Das Handy wird nämlich von den Strafverfolgungsorganen de facto zu einem Peilsender umfunktioniert (s.o.), ohne dass dem Benutzer dieses bekannt ist oder er gar – im Gegensatz zu seinem Gesprächsverhalten am Telefon – Einfluss darauf hätte. Die Erfassung der Positionsdaten anhand des Mobilfunkverkehrs im Stand-by-Betrieb und die damit verbundene Möglichkeit der Erstellung eines Bewegungsprofils ist somit nach geltendem Recht schlicht rechtswidrig.[18]

Die Ortung anhand des GPS

15 So auch der BGH noch in seiner wegweisenden „Raumgesprächsentscheidung" vom 16.3.1982 (BGH in Strafsachen, Bd. 31, S. 296-302). Dort führt er aus, dass nur die „unmittelbar" mit dem Telefongespräch zusammenhängenden Vorgänge, wie beispielsweise das Anwählen, von § 100a StPO erfasst würden.

16 BGH-Ermittlungsrichter a.a.O. (Fn. 9), S. 215

17 vgl. Wälter, H.; Stienkemeier, B.: Beweissicherung im Ermittlungsverfahren, in: Kriminalistik 1994, H. 2, S. 93-100 (94)

18 ausführlich dazu: Gercke a.a.O. (Fn. 6), Kap. IV G; vgl. auch Bernsmann, K.: Anmerkung zu BGH Ermittlungsrichter, in: Neue Zeitschrift für Strafrecht 2002, H. 2, S. 103f.

Das Global Positioning System (GPS) ist ein vom US-amerikanischen Militär entwickeltes Ortungs- und Navigationssystem, dem mittlerweile die tragende Rolle bei der Lokalisierung von Menschen oder Gegenständen zukommt. Es lässt unabhängig von seiner konkreten Verwendung eine bis auf wenige Meter genaue und ununterbrochene Ortung zu.[19] Bereits seit längerem existieren auch Mobilfunkgeräte mit integriertem GPS-Empfänger, so dass die Lokalisierung direkt an die Hardware gekoppelt wird.[20] Dadurch ist eine wesentlich präzisere Standortbestimmung des Mobilfunkgerätes möglich als durch die „herkömmliche" Funkpeilung, die zunächst – ohne zusätzliche aufwendige Peilmaßnahmen – nur die Bestimmung der Funkzelle zulässt, die in ihrem Ausmaße erheblich divergieren kann. Darüber hinaus geschieht die Ortung via GPS unabhängig von der verwendeten SIM-Karte, da sie bloß an das eigentliche Mobilfunkgerät gekoppelt ist. Und schließlich ist es nicht einmal notwendig, dass das Handy im (Stand-by-)Betrieb ist.

Die Anwendung des GPS auf Grundlage geltenden Rechts ist umstritten. Nach einer Entscheidung des Oberlandesgerichts (OLG) Düsseldorf im sog. AIZ-Verfahren soll der GPS-Einsatz unproblematisch unter § 100c Abs. 1 Nr. 1b StPO fallen, der den Einsatz bestimmter technischer Mittel für Observationszwecke erlaubt.[21] Bei der Verabschiedung dieser Norm dachte der Gesetzgeber jedoch an die klassischen Observationsmittel wie Peilsender oder Nachtsichtgeräte.[22] Ob sich der GPS-Einsatz mit solchen Mitteln vergleichen lässt, ist schon angesichts seiner technischen Funktionsweise mehr als fraglich.[23] Bedenken gegen die Rechtmäßigkeit des GPS-Einsatzes ergeben sich darüber hinaus vor allem aus dem Umstand, dass sich deutsche Strafverfolgungsbehörden eines Mittels des US-Militärs bedienen. Hier ist insbesondere die weltraumrechtliche Komponente zu beachten: Aus allen einschlägigen UN-Resolutionen und Verträgen ergibt sich, dass der Weltraum kein rechtsfreier Raum ist und ausschließlich zu „friedlichen Zwecken" genutzt werden darf. Ob nun ein Einsatz zu repressiven staatlichen Überwachungszwecken noch als „peaceful purpose" i.S.d. Art. 4 Abs. 2 des Weltraumvertrages anzusehen ist,

19 zur Funktionsweise des GPS: http://gibs.leipzig.ifag.de
20 s. Woznicki, K.: Handliches Mapping, www.telepolis.de/deutsch/inhalt/te/5688/ 1.html
21 OLG Düsseldorf, in: Neue Zeitschrift für Strafrecht 1998, H. 5, S. 268-270
22 BT-Drs. 12/989 v. 25.7.1991, S. 39
23 vgl. Comes, H.: Der Fluch der kleinen Schritte, in: Strafverteidiger 1998, H. 10, S. 569-573

erscheint zumindest zweifelhaft.[24] Der BGH hat jedoch auch hier keine Bedenken und hat die Entscheidung des OLG Düsseldorf in einem Urteil vom 24.1.2001 im Wesentlichen bestätigt.[25]

„Wunderbox“ IMSI-Catcher

Bei IMSI-Catchern handelt es sich um Geräte, die die feste Basisstation eines Mobilfunknetzes simulieren. Jedes eingeschaltete Handy im Empfangsbereich bucht sich daher in die vermeintliche Funkzelle des IMSI-Catchers ein. Dabei erfasst das Gerät auch die Identitätsnummer des Mobilfunkgerätes (International Mobile Subscriber Identity – IMSI).

Aufgrund der IMSI-Kennung ist zum einen eine Identifikation des Mobilfunkteilnehmers möglich, anhand derer bei Vorliegen einer Abhöranordnung nach § 100a StPO beim jeweiligen Mobilfunknetzbetreiber die zugehörige Rufnummer erfragt werden kann.

Darüber hinaus ermöglicht der IMSI-Catcher auch die Weitervermittlung aller Telefonate, indem er sich gegenüber dem Mobilfunknetz wie ein Handy selbst verhält. So können Mobilfunkgespräche – jedenfalls unter Anwendung einer entsprechenden Zusatzsoftware – direkt vor Ort abgehört werden: ohne Mitwirkung des Mobilfunkbetreibers und damit letztlich auch ohne richterliche Anordnung nach § 100a StPO.[26]

Der Einsatz eines IMSI-Catchers betrifft jedoch nicht nur die eigentlich Verdächtigen, sondern bis zur Erfassung der gesuchten IMSI-Nummer auch alle anderen Mobilfunknutzer, die sich in der simulierten Funkzelle befinden – und zwar die TeilnehmerInnen aller Mobilfunknetze gleichermaßen. Dabei werden zumindest kurzfristig auch Teile des jeweiligen Mobilfunknetzes lahmgelegt. In den vergangenen drei Jahren soll diese „Wunderbox“ – so der „Spiegel“ unter Bezug auf nicht genannte offizielle Quellen – rund dreißigmal eingesetzt worden sein.[27]
Bislang fehlte für den Einsatz des Geräts jegliche rechtliche Spezialermächtigung. Zwar hatte der Bundesrat die damalige Bundesregierung schon am 4.7.1997 aufgefordert, durch Änderung des G10-Gesetzes wenigstens den Nachrichtendiensten den Einsatz des IMSI-Catchers zu

24 Bernsmann, K.: Anmerkung zu BGH, in: Strafverteidiger 2001, H. 7, S. 382-386
25 BGH, in: Strafverteidiger 2001, H. 4, S. 216-219
26 Löwnau-Iqbal, G.: Der Einsatz des „IMSI-Catchers“ zur Überwachung von Handys, in: Datenschutz und Datensicherheit 2001, H. 10, S. 578
27 Spiegel Nr. 33 v. 13.8.2001

ermöglichen; eine solche Regelung lehnte jedoch die rot-grüne Regierung lange Zeit ab. Sie wurde erst mit dem Terrorismusbekämpfungsgesetzes Ende letzten Jahres geschaffen. Der darin enthaltene neue § 9 Abs. 4 Bundesverfassungsschutzgesetz (BVerfSchG) erlaubt dem Inlandsgeheimdienst den Einsatz des IMSI-Catchers unter den relativ strengen Voraussetzungen des § 3 Abs. 1 des G-10-Gesetzes. Überdies unterliegen die Daten unbeteiligter Dritter, die bei diesem Einsatz zwangsläufig anfallen (s.o.), einem absoluten Verwendungsverbot und sind unverzüglich zu löschen.

Für das – im Vergleich zum doch recht speziellen Anwendungsbereich des BVerfSchG – wesentlich alltäglichere Strafverfahrensrecht fehlt jedoch nach wie vor eine ausdrückliche Ermächtigungsgrundlage: Nahezu die gesamte juristische Fachwelt wie auch die Praktiker der Strafverfolgung sind der Ansicht, dass der Einsatz des IMSI-Catchers nicht durch geltendes Strafverfahrensrecht gedeckt sei. An diesem Punkt besteht eine sonst ungewöhnliche Eintracht, die vom Bundesdatenschutzbeauftragten über die Justizminister der Länder bis hin zur Generalstaatsanwaltschaft Celle reicht.[28] Nicht so jedoch die Bundesregierung, allen voran Innenminister Otto Schily: Sie stützt den Einsatz des IMSI-Catchers wiederum auf den § 100a StPO sowie zusätzlich (!) auf die umstrittene „begrenzte Generalklausel“ des § 161 StPO: Dies ist schon deswegen fragwürdig, weil eine Generalklausel grundsätzlich dann subsidiär ist, wenn speziellere Ermächtigungsgrundlagen, wie der § 100a StPO eine ist, vorhanden sind. Gleichwohl erwägt die Bundesregierung aus „Gründen der Rechtssicherheit und -klarheit die Schaffung einer ausdrücklichen Rechtsgrundlage der StPO.“[29] Sie gesteht damit letztlich ein, dass die Subsumtion des Einsatzes von IMSI-Catchern unter die Norm des § 100a StPO nicht dem verfassungsrechtlich erforderlichen Bestimmtheitsgrundsatz gerecht wird. Zwar hatten die Strafsenate des BGH sich bisher noch nicht mit der Zulässigkeit des Einsatzes von IMSI-Catchern zu befassen; die jüngeren Entscheidungen zur Zulässigkeit heimlicher Ermittlungsmaßnahmen insbesondere im Telekommunikationsbereich lassen jedoch befürchten,

28 ebd.

29 BT-Drs. 14/6885, S. 1f.; die Notwendigkeit „begrenzter Generalklauseln“ im Strafprozessrecht versucht die Bundesregierung im Entwurf des Strafverfahrensänderungsgesetzes 1999 herzuleiten, BT-Drs. 14/1484, S. 16

dass das Gericht auch diesbezüglich statt einer grundrechtsfreundlichen eine extensive Auslegung vornehmen wird.

Resümee

Dass sich technische Entwicklungen zwangsläufig auf Gesetzgebung und Rechtsauslegung auswirken, ist eine Binsenweisheit. Dass technikbezügliche Gesetze schon bei ihrer Verabschiedung von den tatsächlichen technologischen Entwicklungen überholt worden sind, ist ebenfalls keine neue Erkenntnis. Dies darf jedoch schon angesichts des Bestimmtheitsgrundsatzes und des hohen Stellenwertes der Grundrechte nicht dazu führen, dass die bloße Existenz neuer Überwachungstechniken auch zwangsläufig zu ihrer Anwendung führt. Dies würde einen sorglosen Umgang mit den tatsächlichen technologischen Möglichkeiten bedeuten, der an sich schon längst überholt geglaubt war.[30] Orientiert man sich lediglich an den realen existierenden Überwachungstechnologien, so erscheint Orwells „1984“ dagegen als naiv-simple „Versuchsversion“.[31]

Dr. Björn Gercke arbeitet am Kriminalwissenschaftlichen Institut der Universität Köln. Seine Dissertation „Bewegungsprofile anhand von Mobilfunkdaten im Strafverfahren“ erscheint in Kürze bei Duncker & Humblot (Berlin).

30 vgl. Bernsmann a.a.O. (Fn. 24), S. 385

31 Sack, F.; Nogala, D.: Überwachungstechnik im Dienst der Polizei, in: Bäumler, H. (Hg.): Polizei und Datenschutz, Neuwied 1999, S. 199-214 (200)

Internet-Streifen

Recherchen ohne Verdacht im weltweiten Datennetz

von Martina Kant

Virtuelle „Streifenfahrten“ im Internet gehören mittlerweile zu den Standardmaßnahmen beim Bundeskriminalamt (BKA), bei der bayerischen Polizei und den Verfassungsschutzbehörden. Unausgesprochenes und auch unerreichbares Ziel dabei ist es, sämtliche Äußerungen im World Wide Web, im Chat und in Newsgroups auf ihre strafrechtliche Relevanz bzw. „Verfassungsfeindlichkeit“ zu überprüfen.

Bereits seit dem 1. Februar 1995 werten PolizeibeamtInnen des bayerischen Landeskriminalamts (LKA) und des Polizeipräsidiums München anlassunabhängig das Internet nach strafbaren Inhalten aus. Nach einem vierjährigen Pilotprojekt wurde das Sachgebiet „Netzwerkfahndung“ im Februar 1999 als dauerhafte Zentralstelle für Bayern mit neun BeamtInnen beim LKA angesiedelt. Wie uns die Pressestelle des Polizeipräsidiums München Ende März mitteilte, recherchieren auch neun BeamtInnen des dortigen Kommissariats 343 weiterhin ohne Anlass im Netz.

Während Bayerns Innenminister Günther Beckstein gefordert hatte, auch in den anderen Bundesländern polizeiliche Stellen zur Internet-Recherche einzurichten, beschloss die Innenministerkonferenz im November 1998 statt dessen, dass das BKA als Zentralstelle diese Aufgabe übernehmen sollte. Im März 1999 nahm schließlich die „Zentralstelle für anlassunabhängige Recherchen in Datennetzen“ (ZaRD) beim BKA ihre Arbeit auf. Nach Auskunft der BKA-Pressestelle sind derzeit für den Bereich der sog. Staatsschutzdelikte acht BeamtInnen in der Staatsschutzabteilung in Bonn-Meckenheim beschäftigt. Die zwölf BeamtInnen der Wiesbadener Dienststelle befassen sich bei ihren Recherchen mit der übrigen Kriminalität im Internet.

Ermittlungsschwerpunkt Kinderpornografie

Im Zentrum der anlasslosen Recherchen steht sowohl in Bayern als auch beim BKA die Suche nach kinderpornografischem Material und dessen Anbietern. Dieser Schwerpunkt schlägt sich jedenfalls in den Statistiken über Verdachtsfälle nieder. Die Übersicht gibt weniger Aufschluss über die „Kriminalität im Netz", sondern sagt eher etwas über die Arbeitsweise der Polizei aus: Gefunden wird, wonach auch gesucht wird.

Da das BKA eigens eine Gruppe für die Suche nach Staatsschutzdelikten ins Netz schickt – nach eigenen Angaben mit dem Tätigkeitsschwerpunkt Rechtsextremismus –, ist die Zahl der Verdachtsfälle in diesem Bereich entsprechend höher als bei den bayerischen Polizei-Surfern.

Tab. 1: Verdachtsfälle bei anlassunabhängigen Internet-Recherchen[1]

	LKA Bayern			BKA		
	2001	2000	1999	2001	2000	1999
Kinderpornografie	407	409	416	903	1117	1008
sonst. Sexueller (Kindes-)Missbrauch	4	36	17	6	13	5
Tier-/Gewaltpornografie	22	58	90	20	70	15
Pornografie/Jugendschutz	104	143	129	1	1	6
BtMG				11	18	17
Arzneimittelgesetz				36	37	27
Wirtschafts- u. Computerkriminalität	5	12	6	12	14	21
Urheberschutz				1	11	7
sonstige Delikte	39	21	21	7	7	12
Staatsschutzdelikte	5	19	17	89	243	8[2]
davon Linksextremismus	0	0	1			
davon Rechtsextremismus	5	19	16			
Verdachtsvorfälle gesamt	586	698	696	1086	1531	1126
davon aufgrund von Eigenrecherchen	411	471	411	1086	1531	1126
davon aufgrund von Hinweisen Dritter	285	281	285			

1 Die Angaben aus Tabelle 1 und 2 stammen jeweils aus einer schriftlichen Auskunft der bayerischen LKA- und der BKA-Pressestelle an die Redaktion.

2 In der Zeitschrift Die Polizei 1999, H. 9, S. 265 sind als erste Bilanz des BKA von Mitte Juni 1999 96 Fälle aus dem Bereich Staatsschutz genannt (davon Linksextremismus: 40, Rechtsextremismus: 22, politisch motiv. Ausländerkriminalität: 18, sonst. Delikte: 16).

Andere internettypische Deliktsbereiche wie Urheberrechtsverstöße und bestimmte Betrugsformen bleiben hingegen weitgehend unberücksichtigt. Die Polizei sieht sich schlicht überfordert, das gesamte Netz konzentriert und systematisch auch nach anderen Delikten zu durchsuchen.[3] Mittlerweile haben die Landeskriminalämter Online-Meldestellen eingerichtet, an die SurferInnen ihre Beobachtungen über verbotene Pornografie, Volksverhetzung usw. der Polizei schicken können.[4] Ob allerdings das Online-Denunziantentum die Polizei entlastet, darf bezweifelt werden: Nach Auskunft des bayerischen LKA betrafen von den 4.572 Hinweisen, die es im Jahr 2001 erhielt, rund 63 % keine strafrechtlich relevanten Inhalte, knapp 30 % waren der Polizei bereits bekannt.

Strategien und Ermittlungsmethoden

Die bayerischen „Netzwerkfahnder" begannen 1995 zunächst damit, die Angebote der Mailboxen zu kontrollieren. Mittlerweile durchsuchen die PolizeibeamtInnen prinzipiell alle Dienste des weltweiten Datennetzes. Die Suche nach illegalen Inhalten im WWW über allgemeine Suchmaschinen wie Google oder Altavista sei aber wenig effizient, erbringe zu viele Treffer und oft nur vermeintlich illegale Inhalte, mit denen die Website-Betreiber Aufmerksamkeit erwecken wollten. Daher recherchiert die Polizei dort, wo sie „Treffer" vermutet. Das seien bei der Suche nach indizierten rechtsextremen Musiktiteln Filesharing-Börsen (z.B. Napster) oder bei der Suche nach Kinderpornografie vor allem einschlägige Diskussionsforen im Usenet sowie Chat-Räume. Dort habe es immer wieder Hinweise auf tatsächliche illegale Web-Seiten gegeben.[5]

Die bayerischen Fahnder würden dabei gezielt nach PC-Usern suchen, die „in den Foren bzw. über Passwortkontakte pornografische Bilder und Texte tauschen, Pornografie auf Videos und sonstigen Datenträgern zum Kauf anbieten, sexuelle Dienste gegen Geld offerieren (Hostessen), ... Typen, die Minderjährige an Pädosexuelle gegen Bezahlung zu vermitteln versuchen." Polizeilich interessant seien auch „diejenigen, die

3 vgl. Fiehl, H.: Erfahrungen bei der Recherche in den Datennetzen, in: der kriminalist 1999, H. 1, S. 2-6 (2)

4 s. die Liste unter: www.heise.de/ct/Netz_gegen_Kinderporno/meldestellen.shtml

5 Steiger, A.; Adler, Ch.: Auf Streife, in: Deutsches Polizeiblatt 2001, H. 4, S. 23-25 (24)

als sog. Verbalerotiker Bildschirmdialoge führen, und natürlich auch Personen, die Privatkontakte mit sexueller Erwartung suchen."[6]
Mit diesem „Raster" dürfte die Polizei weit über das Ziel hinausschießen. Problematisch an diesem Vorgehen ist insbesondere, dass auch Äußerungen und sexuelle Neigungen in den Blickwinkel der Ermittler geraten, die strafrechtlich vollkommen irrelevant sind.

Tab. 2: „Tatorte" der Verdachtsfälle

	LKA Bayern			BKA		
	2001	2000	1999	2001	2000	1999
Chat / IRC / ICQ	8	15	122	342	ca. 600	667
World Wide Web (WWW)	522	489	368	281	ca. 230	194
Usenet / Newsgroups	16	64	142	468	ca. 500	189
E-Mail-Bereich[7]	32	129	63			136
File-Sharing-Networks / FTP	8	1	1	15		4
Sonstige	-	-	-	10		2

Beim bloßen Beobachten offener Kommunikation bleibt es jedoch nicht. Die BeamtInnen des PP München versuchen zum Beispiel im Internet Relay Chat (IRC), einem Dienst, der Online-Kommunikation in Echtzeit über die Tastatur ermöglicht, gezielt mit Anbietern und Empfängern von Pornografie in Kontakt zu kommen. Stammt der Anbieter aus dem Raum München, gehen sie zum Schein auf Angebote zum Tausch von Kinderpornografie ein, ansonsten leiten sie ihre Ergebnisse an die zuständige Polizeidienststelle weiter. Ist der Anbieter zu einem Treffen bereit, schlägt die Polizei beim Austausch des Materials zu.[8]

Anders als die Länderpolizeien kann das BKA in diesen Fällen grundsätzlich nicht selbst aktiv werden. Stoßen die BeamtInnen auf verdächtiges Material, versuchen sie lediglich den Urheber zu ermitteln und geben die Daten an das zuständige LKA.

Überwachung politischer AktivistInnen

6 Fiehl a.a.O. (Fn. 3), S. 3

7 Nach Auskunft des BKA erfasst es darunter alle Fälle, bei denen bei Entdeckung nur eine E-Mail-Adresse des möglichen Urhebers bekannt ist. Diese Erklärung überzeugt nicht, da auch für diese Fälle ein „Tatort" zutreffen müsste. Vermutlich handelt es sich hierbei um E-Mails, die die Polizei selbst als (nicht offen ermittelnde) Beamte erhalten hat.

8 Süddeutsche Zeitung v. 11./12.11.1995

Nicht nur die Polizei überwacht das Internet. Auch die Verfassungsschutzämter beobachten die Internet-Aktivitäten auf sogenannte verfassungsfeindliche Bestrebungen. Bekannte Homepages „mit extremistischen Inhalten“ werden regelmäßig auf Aktualisierungen überprüft, bei Internet-Recherchen neu entdeckte „extremistische“ Seiten wertet der Verfassungsschutz systematisch aus.[9] Die Ergebnisse finden sich in den Verfassungsschutzberichten wieder, die in den letzten Jahren um Kapitel zu Internetaktivitäten ihrer Klientel erweitert wurden. Hinweise auf festgestellte strafbare rassistische, antisemitische oder extremistische Inhalte geben die Ämter an die Polizei weiter. In welchem Umfang die Verfassungsschutzbehörden das Internet als Informationsquelle über Aktivitäten und Äußerungen einzelner Personen heranziehen und diese Daten speichern, kann nur gemutmaßt werden.

Im Vorfeld des EU-Gipfels in Göteborg und des G-8-Treffens in Genua „wurden seitens der deutschen Sicherheitsbehörden fortlaufend Internetrecherchen durchgeführt“, teilte das Bundesinnenministerium auf eine parlamentarische Anfrage hin mit.[10] Konkrete Aufrufe zur Beteiligung an Straftaten hat die Polizei dabei in keinem Fall gefunden. Alle Ergebnisse, insbesondere Angebote für Fahrten nach Göteborg, wurden jedoch registriert und den schwedischen Sicherheitsbehörden „fortlaufend“ übermittelt.[11] Betroffen von den Überprüfungen waren u.a. die Seiten www.fau.org der anarchosyndikalistischen „Freien ArbeiterInnen Union“ (FAU-IAA), www.sav-online.de der Sozialistischen Alternative oder das Mediennetzwerk www.de.indymedia.org.

Auch in Spanien wurden Web-Seiten von GlobalisierungsgegnerInnen Ziel systematischer Überwachungen durch spanische Sicherheitsbehörden. Schon Monate vor dem EU-Gipfel in Barcelona Mitte März dieses Jahres registrierten die BetreiberInnen der linken Internet-Plattform www.nodo50.org vermehrt Zugriffe durch Computer der Guardia Civil, der Policía Nacional und des spanischen Innenministeriums.[12] Anhand der IP-Adressen, die im Server-Logfile gespeichert werden, konnte nicht nur die Netzzugehörigkeit der Rechner identifiziert werden, sondern auch, was die staatlichen Surfer auf den Seiten der über 400 Organisatio-

9 BT-Drs. 14/2879 v. 10.3.2000, S. 7 (schriftliche Antwort der Bundesregierung)
10 BT-Plenarprotokoll 14/178 v. 27.6.2001, S. 17509, 17540
11 ebd., S. 17509
12 s. http://losvigilantes.nodo50.org/infoenglish.html

nen bei nodo50 interessierte. Sie suchten zum einen gezielt nach Terminen, Aktionen und Treffpunkten der Anti-Globalisierungsbewegung, und zum anderen versuchten sie sich unter Pseudonymen in Mailing-Listen einzuschreiben – das misslang allerdings, da sie ungültige E-Mail-Adressen angaben. Über die Medien suggerierte die spanische Polizei, sie wüsste alles über die Anti-Globalisierungsbewegung – was sie denkt, was sie tut, was sie diskutiert. Nodo50 hat daraufhin kurzerhand den Zugriff für die Computer der Sicherheitsbehörden gesperrt.

Automatisierung der Web-Überwachung

Seit Mitte vergangenen Jahres steht den deutschen Polizei- und Verfassungsschutzbehörden das „Internet-Ermittlungstool", kurz INTERMIT zur Verfügung, das die Fahndungsarbeit gezielter, schneller und damit effizienter gestalten soll. Das vom Bundesamt für Sicherheit in der Informationstechnik entwickelte Werkzeug war vom Bundesinnenministerium noch unter Manfred Kanther in Auftrag gegeben worden. Im Kern sei es eine Meta-Suchmaschine, mit der „weitgehend automatisiert und systematisch das Internet nach verbotenen Inhalten wie etwa rechtsextremistischen oder kinderpornografischen Seiten" durchsucht werden könne.[13] Die Software könne Wörter und Begriffe analysieren und würde „Treffer" in einer Unix-Datenbank ablegen. Die Anwendung sei auf das WWW beschränkt; E-Mail- oder Chat-Kommunikation werde nicht gescannt.[14] Beim BKA und bayerischen LKA befindet sich INTERMIT noch in der Erprobungsphase. Ein regelmäßiger Einsatz im Rahmen der anlassunabhängigen Recherchen findet nach Auskunft des BKA noch nicht statt. Neben Fragen der Effizienz – trotz der Technik ist mit einer Vielzahl von Treffern zu rechnen, die gesichtet werden müssen – ist bislang völlig unklar, auf welcher Rechtsgrundlage Polizei und Geheimdienste das gesamte Web scannen dürfen.

Für die Suche nach Kinder- und Tierpornografie kommt beim BKA und den LKÄ seit 1998 die Software PERKEO zum Einsatz.[15] Mit diesem Daten-Scanner können beliebige Datenträger (lokal, im Netzwerk, News-Server oder Webspace) durchsucht und Dateien mit pornografischen

13 Pressemitteilung des BSI v. 16.5.2001, www.bsi.bund.de/presse/archiv/intermit.htm

14 vgl. www.heise.de/tp/deutsch/inhalt/te/7690/1.html

15 PERKEO = **P**rogramm zur **Er**kennung **k**inderpornografischer **e**indeutiger **O**bjekte, s. www.perkeo.net; vgl. www.heise.de/tp/deutsch/inhalt/te/1520/1.html

Bildern anhand der Prüfsummen von zuvor identifizierten Bildern gefunden werden. Darin liegt aber gerade die Schwäche, denn PERKEO kann lediglich Duplikate finden; wird nur ein Bit der Datei verändert, sinkt die Trefferquote auf Null.

Rechtliche Grauzone

Das einfache verdachtslose Surfen in öffentlichen Bereichen des Datennetzes wird sowohl von der Polizei als auch von JuristInnen und DatenschützerInnen zunächst *nicht* als Grundrechtseingriff gewertet, sondern als Informationsbeschaffung aus allgemein zugänglichen Quellen – vergleichbar mit der Auswertung von Zeitungen, Zeitschriften, Filmen usw. nach strafbaren Inhalten.[16] Dieses sei durch die Aufgabenzuweisungen in den Polizeigesetzen (Gefahrenabwehr, vorbeugende Bekämpfung von Straftaten) abgedeckt. Für Internet-Recherchen, mit denen Lagebilder oder andere allgemeine Einschätzungen ohne direkten Personenbezug – z.B. über die Zahl rechtsextremistischer Web-Seiten – gewonnen werden sollen, mag dies zutreffen. Sobald aber im Netz gezielt nach Daten bestimmter Personen gesucht wird, bei den Recherchen personenbezogene Daten erhoben werden oder Polizeibeamte verdeckt an Diskussionsforen oder Chats teilnehmen, greift dies in das Recht auf informationelle Selbstbestimmung ein und bedarf einer rechtlichen Grundlage.

Für das Bundeskriminalamt heißt dies, dass verdeckte, die polizeiliche Identität bewusst verheimlichende oder verschleiernde Recherchen im Internet *rechtswidrig* sind, da das BKA-Gesetz keine Ermächtigungsgrundlage dafür darstellt. Nach § 2 Abs. 1 i.V.m. § 7 Abs. 2 BKA-Gesetz dürfen die BeamtInnen nur *offen* Daten bei nicht-öffentlichen Stellen erheben. Auf die Regelungen der Strafprozessordnung kann sich das BKA in diesem Stadium der Beobachtung – ein Verdacht liegt bei den anlasslosen Recherchen gerade nicht vor – auch nicht stützen.[17]

Um offen zu ermitteln, muss die Polizei, wenn sie einen Chat-Raum betritt oder an einem Diskussionsforum teilnimmt, ihre Behördeneigen-

16 vgl. hierzu bspw. Bär, W.: Auf dem Weg zur „Internet-Polizei“?, in: Bäumler, H. (Hg.): Polizei und Datenschutz. Neupositionierung im Zeichen der Informationsgesellschaft, Neuwied, Kriftel 1999, S. 167-187 (170)

17 vgl. Bundesbeauftragter für den Datenschutz: 18. Tätigkeitsbericht (1999-2000), BT-Drucksache 14/5555 v. 13.3.2001, S. 105

schaft deutlich machen, ansonsten ermittelt sie verdeckt.[18] Dass das BKA sich bei seinen Recherchen im Chat und Usenet als BKA zu erkennen gibt, muss angesichts der hohen Fallzahl (s. Tab. 2) bezweifelt werden.

Auch die bayerische Polizei bewegt sich bei ihren virtuellen Streifen in einer rechtlichen Grauzone. Denn fraglich ist, ob sie sich bei ihren verdeckten Einsätzen im Chat oder Usenet unter Verwendung von Pseudonymen auf die Bestimmungen des Polizeiaufgabengesetzes (PAG) über die Datenerhebung (Art. 31) oder Datenerhebung mit besonderen Mitteln (Art. 33) berufen kann. Zum einen unterscheidet sich diese Form der Datenerhebung erheblich von herkömmlichen Streifenfahrten, Recherchen oder der beobachtenden Teilnahme an Veranstaltungen. Jede Veröffentlichung im Internet ist auf Dauer abrufbar und ohne Probleme dauerhaft speicherbar, jede Äußerung im Diskussionsforum oder Chat kann mitgeschnitten und einer bestimmten Person zugeordnet werden. Verdachtslose Internetstreifen sind daher eher vergleichbar mit Streifenfahrten mit optionaler Videoaufzeichnung oder – im Falle der Chat-Kommunikation – dem verdeckten Einsatz technischer Mittel zur Aufzeichnung des nichtöffentlich gesprochenen Wortes oder dem Einsatz Verdeckter Ermittler. Deren Einsatzvoraussetzungen knüpfen jedoch im PAG an eine konkrete Gefahr für schwerwiegende Rechtsgüter (Leib, Leben, Sicherheit des Bundes etc.) oder den Anfangsverdacht einer bevorstehenden „Straftat von erheblicher Bedeutung“ an; beides ist bei anlassunabhängigen Internetrecherchen nicht ohne weiteres gegeben.

Totale Überwachung?

Dass die Polizei „die Kriminalität im Internet“ in den Griff bekommt, glaubt sie nicht einmal selbst (vermutlich deshalb setzt sie bei der Internet-Streife in erster Linie auf Abschreckung[19]). Auch die Forderung der Deutschen Polizeigewerkschaft nach 5.000 weiteren Stellen für Polizei-Surfer wird daran nichts ändern. Alarmieren muss allein schon das staatliche Bestreben, das weltweite Datennetz unter Kontrolle bringen zu wollen. Die Bekämpfung von Kinderpornografie ist dabei nur der Türöffner, der die Legitimation für die Totalüberwachung des Internet schaffen soll. Wenn schließlich die InternetnutzerInnen befürchten müssen, dass

18 vgl. Germann, M.: Gefahrenabwehr und Strafverfolgung im Internet, Berlin 2000, S. 520
19 s. Die Polizei 1999, H. 9, S. 265

die Polizei wahllos, verdeckt und unter Verwendung von spezieller Software alle jemals geäußerten Netz-Inhalte beobachtet, sind Meinungsfreiheit und Meinungsvielfalt massiv bedroht.

Martina Kant ist Redakteurin von Bürgerrechte & Polizei/CILIP.

Ohne Technik läuft nix

Auf dem Weg zur automatischen Überwachung

von Erich Moechel und Nick Lüthi[1]

Praktisch zeitgleich sind Anfang 2002 in Deutschland, Österreich und der Schweiz neue Abhörverordnungen in Kraft getreten.[2] Dahinter zeigen sich Bestrebungen, europaweit verbindliche technische Standards zu etablieren, die eine lückenlose und quasi automatisierte Überwachung sämtlicher Telekommunikationsnetze ermöglichen. Die Standardisierungsbestrebungen werden insbesondere innerhalb des European Telecommunications Standards Institute (ETSI) vorangetrieben und erfolgen seit 1992 auf Initiative der US-Bundespolizei FBI und der EU.

Es begann vor neun Jahren: Die „International User Requirements", die bis heute als Agenda für die konkreten technischen und politischen Umsetzungen der Telekommunikationsüberwachung figurieren, reichen bis in das Jahr 1993 zurück. Im ersten einer Reihe der so genannten „International Law Enforcement Telecom Seminars" (ILETS) einigten sich die Nachrichtendienste und die Polizei der ECHELON-Betreiber USA, England, Kanada und Australien mit den wichtigsten EU-Staaten auf ein gemeinsames Vorgehen in Fragen der Überwachung von Kommunikati-

1 Der folgende Artikel über die ETSI-Standards beruht auf umfassenden Recherchen von Erich Moechel: Lauschangriff. Abhörstandards für Europa, in: c't 2001, H. 7, S. 58; s.a. www.heise.de/tp/deutsch/special/enfo/7220/1.html; die komplette Dokumentation s. www.quintessenz.at/etsi; Nick Lüthi hat die ETSI-Dossiers für CILIP zusammengefasst.

2 zur deutschen Telekommunikationsüberwachungsverordnung siehe in diesem Heft, S. 19; Schweiz: Verordnung betr. die Überwachung des Post- und Fernmeldeverkehrs, in: Systematische Sammlung des Bundesrechts SR 780.11; Österreich: Verordnung über die Überwachung des Fernmeldeverkehrs, www.quintessenz.at/archiv/msg01419.html

onsnetzwerken. An der FBI-Akademie in Quantico im US-Bundesstaat Virginia wurde ein Papier erstellt, das „Internationale Abhöranforderungen“ (International Requirements for Interception) der Nachrichtendienste formulierte. Zentrale Aussage: Die „gesetzlich ermächtigten Behörden“ benötigen Zugriff auf den Telekommunikationsverkehr in Echtzeit rund um die Uhr. Dies sei nur durch permanente Verbindung der Dienste mit standardisierten Andockstellen in den Netzen möglich.

Bei weiteren, ebenso geheimen ILETS-Treffen (Bonn 1994, Canberra 1995) wurde das Vorgehen bereits mit Vertretern aller EU-Staaten abgesprochen; die „Abhöranforderungen“ mutierten zu „Benutzeranforderungen“ (International User Requirements, IUR). In den USA liefen die IUR 1994 unter dem Titel CALEA (Communications Assistance Law Enforcement Act) nach teilweise heftigen Diskussionen leicht modifiziert durch den Kongress und wurden vom damaligen Präsidenten Bill Clinton abgesegnet. Wenig später, am 17. Januar 1995, wurden sie auch zu einer Entschließung des (Minister-)Rates der EU erhoben. Diese beruhte auf einer Serie von Dokumenten der Arbeitsgruppe Polizeiliche Zusammenarbeit (Kürzel: ENFOPOL) des Rates der Innen- und Justizminister. Beschlossen wurde sie ohne jede Anhörung und Diskussion als „akkordierte Angelegenheit“: Die Innen- und Justizminister hatten im „schriftlichen Verfahren“ zugestimmt. Der Beschluss wurde dem Rat der für Fischerei-Fragen zuständigen Minister als so genannter A-Punkt vorgelegt. Da A-Punkte bei jedem beliebigen Ratstreffen abgesegnet werden können, war das formal korrekt – mehr aber nicht.

Veröffentlicht wurde dieser fait accompli erst 19 Monate später, im November 1996.[3] Aber auch dies fiel den Abgeordneten des Europäischen Parlaments (EP) erst auf, als die britische Bürgerrechtsorganisation Statewatch im Januar 1997 die Entschließung im Rahmen eines Berichts über ein geplantes gemeinsames Überwachungssystem von EU und FBI thematisierte und wenig später ein im Auftrag der Technologiefolgen-Abschätzungseinheit des EP (STOA) erstellter Bericht in dieselbe Kerbe schlug.[4] Die dann folgenden empörten Anfragen der EP-Abgeordneten beantwortete die EU-Kommission nur ausweichend; die der Entschlie-

3 Amtsblatt der Europäischen Gemeinschaften Nr. C 329 v. 4.11.1996, S. 1-6

4 EU and FBI global surveillance system, in: Statewatch-Bulletin 1997, no. 1, p. 1-4, weiteres s. unter www.statewatch.org/eufbi/index.html, www.statewatch.org/soseurope.htm; STOA-Bericht: http://jya.com/stoa-atpc-so.htm

ßung zu Grunde liegenden „ENFOPOL“-Dokumente wurden den ParlamentarierInnen nicht ausgehändigt.

Am Parlament und der Öffentlichkeit vorbei

Der Statewatch-Bericht von 1997 bezog sich auf eine neuere Fassung der IUR und zeigte, welche Fortschritte das Projekt seit der Ratsentschließung von 1995 gemacht hatte. Dies und die Aufdeckung der Umstände, wie die IUR am EP vorbei geschleust wurden, sorgten 1997 ebendort für einen Eklat. War es 1995 noch gelungen, die erste Fassung der Benutzeranforderungen klammheimlich zu beschließen, so scheiterte 1998 der zweite Anlauf, mit dem die IUR um das Internet-Protokoll und den Mobilfunkstandard GSM erweitert werden sollten, in letzter Minute unter dem Druck der Öffentlichkeit. Im deutschsprachigen Raum publizierte das Online-Magazin Telepolis im November 1998 eine ganze Serie von Dokumenten der Polizei-Arbeitsgruppe des Rates (die so genannten ENFOPOL-Papiere) im Volltext.[5] Bezeichnenderweise herrschten zunächst Zweifel an der Echtheit der Papiere. Erst nach einem Bericht des britischen Fernsehsenders Channel 4 griffen weitere Medien das Thema auf, „ENFOPOL“ wurde zum Synonym für die drohende Überwachungsunion. In Polizei- und Geheimdienstkreisen wurden die österreichischen Beamten, die das Papier während der Wiener EU-Präsidentschaft verfasst hatten, herb kritisiert.

Im Frühjahr 1999 exerzierten die Kollegen den Österreichern vor, wie man mit Papieren vom Kaliber der IUR umzugehen hatte: Wie schon in der Fassung von 1995 wurde das Papier zweigeteilt. Alle brisanten Punkte wurden aus dem Entwurf eines Ratsbeschlusses eliminiert und verschwanden in einem Annex mit technischen Erläuterungen, der nicht vorgelegt wurde. So blieb von 42 Seiten nur ein sehr abstrakter, vierseitiger Forderungskatalog übrig.[6] Die runderneuerten IUR wurde schließlich statt in der Form eines Ratsbeschlusses der EU wieder am EP vorbei als europäischer Telekommunikations-Standard eingeführt.

Während das EP im Juli 2000 einen speziellen temporären Ausschuss für das vom US-Geheimdienst NSA dominierte Überwachungssy-

5 s. www.heise.de/tp/special/enfo. Es handelt sich vor allem um das Ratsdok. 10951/98 ENFOPOL 98 v. 3.9.1998 sowie dessen zwei Revisionen.

6 Ratsdok. 6715/99 ENFOPOL 19 v. 15.3.1999

stem ECHELON einberufen hat,[7] ist der Aufbau eines völlig anders strukturierten Überwachungssystems quer durch Europa schon sehr weit fortgeschritten. Es wird den Diensten den Zugriff auf die gesamte digitale Sprach- und Datenkommunikation der europäischen Zivilgesellschaft eröffnen. Dies geschieht insbesondere durch die Definierung von technischen Standards entlang den Bedürfniskatalogen von Geheimdiensten und Polizei auf der einen, sowie den Herstellern von Netzwerkinfrastruktur auf der anderen Seite. Das Interesse der Letzteren ist offensichtlich: Neue Standards erfordern neue Gerätschaft.

Gemischte Bilanz

Im August 2001 wurde der unter dem Kürzel ES 201 671 bekannte Überwachungsstandard von den Mitgliedern des European Telecommunications Standards Institute (ETSI) verabschiedet. Noch fehlt ES 201 671 die politische Legitimation durch die EU. In der aktuellen Version sind aber bereits auf technischer Ebene alle notwendigen Schnittstellen zum Abhören durch Strafverfolgungsbehörden und Geheimdienste festgelegt. Den EU-Mitgliedstaaten bleibt es immerhin überlassen, ob sie automatische elektronische oder manuelle Schnittstellen gestatten.

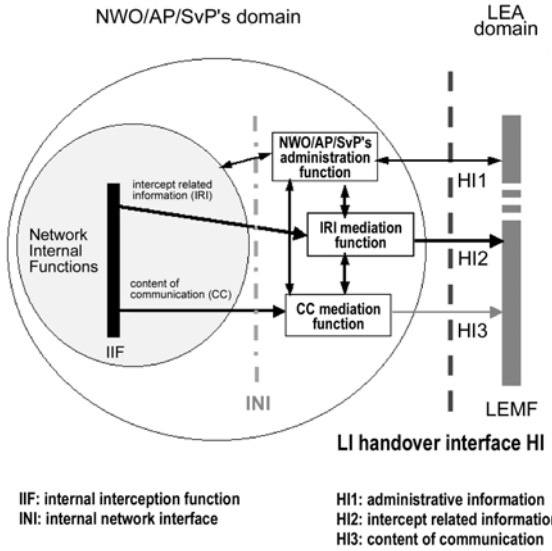
Während im Normalfall die Behörden auf politischer Ebene zunächst generelle Anforderungen formulieren und dann in einem zweiten Schritt die technischen Spezifikationen erarbeitet werden, lief das Verfahren im Fall des Überwachungsstandards ES 201 671 genau umgekehrt. Nachdem die IT-Industrie sich in jahrelangem Ringen mehrheitlich auf einen umfangreichen Schnittstellen-Standard zur Überwachung der digitalen Netze in allen Details geeinigt und damit vollendete Tatsachen geschaffen hatte, wurde das Anforderungspapier der Strafverfolger erst nachgereicht.

Trotz der Verabschiedung von ES 201 671 Version 2.0 als vorläufigem „Zwischenresultat“ der mannigfaltigen Abhörbestrebungen auf EU-Ebene, kann eine Zwischenbilanz keineswegs nur negativ ausfallen. Eine bis dahin völlig ungeniert hinter den Kulissen agierende Gruppe von Verbindungsleuten und Fadenziehern der Polizeien und Geheimdienste kam erstmals an das Licht der Öffentlichkeit. Dazu kommt, dass das lieb-

7 www.europarl.eu.int/committees/echelon_home.htm; siehe auch den Artikel von H. Busch in diesem Heft, S. 49-53

ste Kind der „gesetzlich ermächtigten Behörden“ – so die verharmlosende Umschreibung in den Papieren der Polizeiarbeitsgruppe des Rates –, die vollelektronische Schnittstelle, in der zuletzt veröffentlichten Version von ES 201 671 nicht mehr obligatorisch ist.

Abb.: Modell der Überwachungsschnittstelle nach ES 201 671



Quelle: ETSI ES 201 671 V2.1.1 (2001-09)

NWO: network operator / AP: access provider / SvP's: service provider
LEA: law enforcement agencies / LEMF: law enforcement monitoring facility
LI: lawful interception / HI: handover interface

Über den sogenannten Handover Interface Port HI 1 sind Polizei und Dienste zwar an sich direkt per Standleitung mit der Administrations-Funktion des Netzbetreibers, welche alle Vorgänge an der Schnittstelle kontrolliert, verbunden. Nationalen Regulatoren steht es allerdings nun frei, diese Schnittstelle als manuelles Interface zu gestalten. Der Netzbetreiber kann also darauf bestehen, dass Überwachungsbegehren nicht elektronisch ausgehandelt, sondern auch in Zukunft auf Papier oder persönlich vorgelegt werden.

Grund zur Befürchtung, dass Polizei und Diensten praktisch unbegrenzte Zugriffsmöglichkeiten eingeräumt werden, besteht freilich wei-

terhin. Denn die Möglichkeit der manuellen Übermittlung wurde nicht aus Gründen der Datensicherung gegen Übergriffe vorgesehen. Vielmehr hat die Einführung dieser Verfahrensweise recht prosaische Gründe: Die Gerichte sind europaweit technisch noch nicht in der Lage, ihre Überwachungsanordnungen in sicherer elektronischer Form an die Polizei zu übermitteln, weshalb immer noch Brief- oder Faxverkehr die Regel ist.

Aufträge für die IT-Industrie

Freuen dürften sich trotz dieser Einschränkungen vor allem die IT-Industrie, die in den Gremien des ETSI maßgeblich an der Ausarbeitung des neuen Überwachungsstandards mitgearbeitet hat. Wirklich bedeutende Summen fallen jetzt und in naher Zukunft bei Telecom-Ausrüstern wie Alcatel und Siemens, Ericsson, Nokia, Nortel und anderen an. Wie Ericsson etwa, das ein System namens LIS anbietet, dessen Produktmanager Stefan Björnsson Mitglied der bei der Ausarbeitung des Überwachungsstandards federführenden ETSI-Arbeitsgruppe Lawful Interception ist, haben auch alle anderen Firmen in ihre Produkte – Wählämter und Vermittlungsstellen – mehr oder weniger komplette Überwachungslösungen integriert.

„Hightech speziell für Bedarfsträger“ – so preist Siemens seine „flexible und ausbaufähige Gesamtlösung“ an. „Spezialbeauftragte, die in ihrem Netz Teilnehmerleitungen ‚anzapfen‘? Das ist Vergangenheit!“ Und auch Befürchtungen, dass „eventuell beim Aufschalten erzeugte, Verdacht erregende Leitungsgeräusche den Erfolg Ihrer Überwachungsmaßnahme gefährden“ könnten, sind nunmehr unbegründet, denn „LI arbeitet lautlos“.

Statt „vermittlungstechnisches Sonderequipment“ einzusetzen, das „schwierig zu tarnen“ sei, ließen sich – so verspricht Siemens – Überwachungsaufträge nun mit zusätzlicher Standard-Hardware für sein digitales elektronisches Wählsystem EWSD „unauffällig abwickeln“. Nach Angaben des Konzerns ist dieses Erfolgsprodukt mit über 240 Millionen Ports in 105 Ländern das am weitesten verbreitete System für Sprachtelefonie, jeder fünfte Anruf weltweit erfolge über diese Hardware, die vollständig überwachungstauglich ist. Die Software wiederum verfüge über „spezielle Filterfunktionen für die Materialauswertung“, um „schnell an die wesentlichen Informationen“ zu kommen. „Komfortable Tools“ erleichtern dann die eingehende Analyse des „kompletten, nach Nutzer-

und Ereignisdaten getrennten Informationsflusses aus sämtlichen Aktivitäten an einem überwachten Objekt".

Randdaten interessieren

Den „Bedarfsträgern" geht es dabei nicht nur um Gesprächsinhalte, sondern vor allem um Verkehrs- und Verbindungsdaten, also um die Frage: Wer kommuniziert mit wem, wie häufig, von welchem Standort aus etc.? Der Siemens-Prospekt, der nur im Rahmen eines persönlichen Gesprächs an potenzielle Kunden weitergegeben wird, erklärt dies mit bemerkenswerter Offenheit: „Ereignisdatensätze liefern aufschlussreiche Informationen über das Kommunikationsverhalten des überwachten Netzteilnehmers. Zusammengenommen ergeben all diese Informationen eine Art ‚Verhaltensmuster', das allein oft schon die gewünschten Hinweise liefert, sodass sich das Einholen der Nutzdaten erübrigt."

Internet ist nicht Telefon

Während die Arbeiten am Standard ES 201 671 zur Überwachung von Sprachtelefonie zügig vorankamen, tat man sich bei der Integration des Internet in das Szenario der Überwachung etwas schwer. Die Welt der Datenpakete und des dezentralen Paketverkehrs kommuniziert auf andere und komplexere Weise als das vergleichsweise simple Telefoniemodell, die herkömmlichen „Circuit Switched Networks", die im Grunde nur aus anrufender und angerufener Partei und einem Übertragungskanal besteht. Trotzdem wurde Anfang April 2001 der Entwurf eines ersten Standards präsentiert, der die technische Überwachung des Internet europaweit normieren soll.

Nachdem die grundlegenden Abhörspezifikationen für Telefonienetze aller Art an sich feststehen und nur den jeweils neueren Entwicklungen technischer Art angepasst werden müssen, widmet man sich nun in erster Linie Methoden, den TCP/IP-Verkehr[8] zu erfassen – und zwar „vollständig", „während der gesamten Überwachungsdauer", „möglichst nahe an Echtzeit", dabei „nicht auffällig", nämlich ohne die „Quality of Service" zu beeinträchtigen. Analog zur Überwachung der Telefonie müssen die

8 Daten werden im Internet in einzelnen Datenpaketen „zerhackt" versandt und beim Empfänger wieder zusammengesetzt. Versand, Empfang und Fehlerkontrolle werden über das Transfer Control Protocol (TCP) und das Internet Protocol (IP) gesteuert.

Überwachungsschnittstellen „Multi-User-tauglich“ sein, wobei die parallel angedockten Behörden und Dienste nichts voneinander erfahren dürfen.

Bei einem Treffen verschiedener ETSI Arbeitsgruppen Anfang April 2001 im norwegischen Grimstad hieß es, aus Gründen von „Security und Privacy“ sei ein umfassender Zugriff allerdings „sehr umstritten“ und deshalb für Telekom-Regulatoren in vielen Ländern „höchstwahrscheinlich unakzeptabel“. Damit wurden aber die bereits aus dem 1998 veröffentlichten „Pflichtenheft“ ENFOPOL 98 bekannten, sehr allgemein formulierten Anforderungen, auch den gesamten Internet-Verkehr möglichst in Echtzeit zu erfassen, keineswegs fallen gelassen. Wie das grundlegende Datenmodell zur „IP Interception“ zeigt, wurde nur auf das verzichtet, was realistischerweise ohnehin nicht machbar ist.

Umsetzung geht flott voran

In den Niederlanden hat die Implementierung der Überwachungsschnittstellen bereits seit rund einem Jahr begonnen, Großbritannien hat die politische Umsetzung als „Regulation of Investigatory Powers Act“ (RIP) bereits vollzogen.[9] In Deutschland erweiterten die Parlamentarier bei der Novelle des G 10-Gesetzes auch die Befugnisse des Bundesnachrichtendiensts (BND) zur strategischen Überwachung: Durfte der BND bisher „nur“ die Telekommunikation via Satellit abhören, kann er jetzt auch auf den leitungsgebundenen digitalen Verkehr zugreifen. Dies ist technisch nur durch eine Schnittstelle wie ES 201 671 realisierbar. Im Gespräch mit dem Online-Magazin Telepolis hatte der grüne Abgeordnete Hans-Christian Ströbele kritisiert, das „verfassungskräftige Trennungsgebot zwischen Polizei und Geheimdiensten werde damit weiter aufgeweicht.“ Die Dienste sollten offenbar „als polizeiliche Hilfssheriffs Verdachtsschöpfung betreiben.“[10] Dieses Szenario steht unmittelbar bevor.

Erich Moechel ist Redakteur des österreichischen Online-Magazins futureZone beim ORF. Nick Lüthi arbeitet als freier Journalist in Bern.

9 für Großbritannien siehe Statewatch-Bulletin 2000, no. 1, p. 24f., no. 3-4, p. 12f.; für die Niederlande s. http://cryptome.vwh.net/espy/ES201-671-nl.txt

10 www.heise.de/tp/deutsch/inhalt/te/7194/1.html

Was wird aus den Verkehrsdaten?

Konflikte um EU-Regelungen

von Tony Bunyan

Für Polizeien und Geheimdienste sind die bei der elektronischen Telekommunikation anfallenden Verkehrsdaten verlockende Informationsquellen. Nach einer EG-Richtlinie von 1997 müssen sie aber gelöscht werden, sobald sie nicht mehr für Abrechnungszwecke gebraucht werden. Der Rat, d.h. die Regierungen der EU-Staaten, möchte das ändern und geht auf Kollisionskurs mit dem Europäischen Parlament (EP).

Im Juli 2000 hatte die EU-Kommission einen Vorschlag präsentiert, mit dem die 1997 verabschiedete Richtlinie „über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation" überarbeitet werden sollte.[1] Vorgesehen waren nur Anpassungen an den neuen Stand der Technik, aber keine grundsätzlichen Änderungen. Die Verpflichtung der Telekommunikations- (TK-) Dienstleister, Verbindungsdaten sofort zu löschen, wenn sie für Rechnungszwecke nicht mehr gebraucht werden, sollte erhalten bleiben.

Dieser Vorschlag fand zwar Anklang bei der EG-Datenschutzgruppe und beim EP, nicht aber beim Rat. Die Arbeitsgruppe Polizeiliche Zusammenarbeit des Rats der Innen- und Justizminister macht sich seit Jahren für eine Ausweitung der Überwachung stark. Dazu gehört u.a. die Forderung, dass Anbieterfirmen Verkehrsdaten für einen längeren Zeitraum aufbewahren und den „gesetzlich ermächtigten Behörden" – neben den Polizeien auch den Geheimdiensten – den Zugang hierzu eröffnen sollen. Der Konflikt war damit vorprogrammiert. Da TK-Fragen zur Er-

1 Amtsblatt der Europäischen Gemeinschaften Nr. C365 E v. 19.12.2000; sämtliche hier zitierten Materialien finden sich unter www.statewatch.org/soseurope.htm

sten Säule der EU gehören und für sie das sog. Mitentscheidungsverfahren gilt, war gleichzeitig gesichert, dass das EP nicht nur mitreden kann, sondern auch tatsächlich Einfluss hat.

Nach dem 11. September

Bereits kurz nach den Anschlägen in den USA zeichnete sich ab, dass die Frage der Verkehrsdaten nun auch als Angelegenheit der „Terrorismusbekämpfung" abgehandelt werden sollte. In den „Schlussfolgerungen" seines Sondertreffens vom 20. September ersucht der Rat die Kommission, dafür Sorge zu tragen, „dass die Strafverfolgungsbehörden die Möglichkeit erhalten, im Zusammenhang mit kriminellen Handlungen zu ermitteln, die unter Anwendung elektronischer Kommunikationssysteme begangen wurden." Es gehe, so der Rat, darum, das „Gleichgewicht" zwischen Datenschutz und der „Notwendigkeit des Zugangs der Strafverfolgungsbehörden" zu Verkehrsdaten zu wahren – und zwar wohlgemerkt nicht nur für Zwecke der Terrorismusbekämpfung, sondern allgemein für „strafrechtliche Ermittlungszwecke".[2]

Am 16. Oktober erhielt die EU-Kommission auch Druck aus den USA. In seinem Brief an Kommissionspräsident Romano Prodi verlangt der US-Präsident u.a., die im Richtlinienentwurf vorgesehene zwingende Löschung von Verkehrsdaten zu revidieren und „die Aufbewahrung dieser kritischen Daten für einen angemessenen Zeitraum zu erlauben". Die Forderung ist um so anmaßender, als es in den USA eine entsprechende Regelung nicht einmal im neuen Anti-Terror-Gesetz (US-PATRIOT Act) gibt.

Am 13. November lehnte das EP die Veränderungswünsche des Rates in erster Lesung ab. Am 28. Januar verabschiedete der Rat formell seinen Gemeinsamen Standpunkt, in dem er seine Forderungen bekräftigt. Bereits zwei Tage später nahm die Kommission in ihrer „Mitteilung" an das EP hierzu Stellung.[3] Nach dem Mitentscheidungsverfahren müssen sich Kommission, Parlament und Rat auf einen gemeinsamen Text einigen. Das EP muss eine zweite Lesung durchführen, der Rat wiederum einen

2 Ratsdok. 12156/01 v. 25.9.2001

3 Mitteilung der Kommission an das Parlament v. 30.1.2002, SEK 2002/0124 endg. – COD 2000/0189

Gemeinsamen Standpunkt festlegen. Wenn beide an ihren Positionen festhalten, geht es vor einen Vermittlungsausschuss.

Die Kommission gibt nach

Gestritten wird in erster Linie um Art. 15 Abs. 1 des Richtlinienvorschlags. Schon in der ursprünglichen Fassung erlaubte dieser Artikel den Mitgliedstaaten, nationale Rechtsvorschriften für Eingriffe in das Telekommunikationsgeheimnis inkl. Zugriff auf Verkehrsdaten zu erlassen – und zwar für Zwecke der Landesverteidigung, der nationalen und der öffentlichen Sicherheit sowie für die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten. Das EP hatte in seiner 1. Lesung diese Formulierung erheblich zurückgestutzt: Einschränkende Gesetze der Mitgliedstaaten sollten nur zugelassen sein, soweit das „in einer demokratischen Gesellschaft angemessen, verhältnismäßig, zeitlich begrenzt und notwendig ist. Diese Maßnahmen sollten ganz und gar die Ausnahme darstellen, sich auf eine allgemein verständliche spezifische Rechtsvorschrift stützen und von Gerichten oder anderen zuständigen Behörden von Fall zu Fall genehmigt sein. Gemäß der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten und den Entscheidungen des Europäischen Gerichtshofs für Menschenrechte ist jede Form einer großangelegten allgemeinen oder sondierenden elektronischen Überwachung verboten.“ Eine allgemeine Aufbewahrung von oder Rasterfahndung mit Verkehrsdaten wäre damit ausgeschlossen.

Der Rat schlägt stattdessen folgende Ergänzung vor: „Zu diesem Zweck können die Mitgliedstaaten unter anderem vorsehen, dass die (Verkehrs-)Daten aus den in diesem Absatz aufgeführten Gründen (Landesverteidigung, Nationale Sicherheit etc.) während einer begrenzten Zeit gemäß den allgemeinen Grundsätzen des Gemeinschaftsrechts aufbewahrt werden.“ Damit ist der Grundsatz der Löschung der Verkehrsdaten in Art. 6 der Richtlinie für die „mit dem Schutz der öffentlichen Interessen betrauten Behörden“ aufgegeben. Der Vorschlag macht den Datenschutz im Telekommunikationsbereich wertlos. In der Begründung heißt es, damit würde „das erforderliche Gleichgewicht zwischen den Erfordernissen des Schutzes der Privatsphäre und den Bedürfnissen des für den Schutz der Sicherheit zuständigen einzelstaatlichen Behörden besser

gewährleistet.“ Dies sei wegen der „erheblichen Gefahren, die durch die Ereignisse am 11. September 2001 sichtbar geworden sind,“ nötig.[4]
Bereits auf der Tagung des Telekommunikationsrates am 6. Dezember hatte die Kommission signalisiert, sie sei bereit, ihren Widerstand gegen die vom Rat vorgeschlagenen Änderungen in Art. 6 und 15 Abs. 1 des Entwurfs aufzugeben. Die Datenschutzgruppe hatte darauf mit einer sehr nachdrücklich formulierten Stellungnahme reagiert. „Maßnahmen gegen Terrorismus sollten und dürfen nicht die grundrechtlichen Standards reduzieren, die demokratische Gesellschaften charakterisieren.“ Die aufgrund der Datenschutzrichtlinie von 1995 gebildete Arbeitsgruppe wehrte sich gegen die „zunehmende Tendenz, den Schutz der Privatsphäre als Hindernis eines effizienten Kampfs gegen den Terrorismus darzustellen.“ Die datenschützerische Kritik konnte jedoch nicht verhindern, dass die Kommission in ihrer Mitteilung vom 30. Januar offiziell dem Druck des Rates nachgab. Der Zusatz in Art. 15 sei unbedenklich, er bedeute keine generelle Verpflichtung der Mitgliedstaaten, vom Grundsatz der Löschung von Verkehrsdaten abzuweichen.

Die Kommission ignoriert jedoch, dass alle EU-Regierungen sich für eine generelle Aufbewahrung dieser Daten einsetzen werden, weil (grenzüberschreitende) Überwachung nur funktioniert, wenn es in allen Staaten vergleichbare Befugnisse gibt. Schon vor dem 11. September hatten die Niederlande, Belgien und Frankreich entsprechende Regelungen geplant oder eingeführt. Großbritannien hatte eine „freiwillige Vereinbarung“ in der Schublade, die jetzt durch das Anti-Terror-Gesetz („Anti-terrorism, Crime and Security Act 2001, ATCS“) überholt ist.

In der Erläuterung zum ATCS heißt es: „Daten über eine bestimmte Person, gegen die sich die Ermittlungen richten, werden nur abrufbar sein, wenn Telekommunikationsdaten der gesamten Bevölkerung aufbewahrt werden.“ In ähnlicher Weise will auch die Task Force der Polizeichefs der EU-Staaten den Zugriff auf Verkehrsdaten nicht für spezifische Ermittlungen im Einzelfall, sondern für „Zwecke der Forschung“, für allgemeine Fischzüge ohne konkreten Tatverdacht.

Ob das EP seine ablehnende Position beibehält, wird sich in naher Zukunft entscheiden. Eines ist jedoch bereits jetzt klar: Wenn die grundlegenden Prinzipien über den Datenschutz im Telekommunikationssek-

4 EP-Position in Anlage zu Ratsdok. 13831/01, Ratsposition: Ratsdok. 15396/2/01 Add 2

tor aus der Richtlinie von 1997 jetzt aufgegeben werden, dann sind sie für immer verloren. Die EU ginge damit weiter auf dem autoritären Weg der flächendeckenden Überwachung.

Tony Bunyan ist Herausgeber von Statewatch in London.

Überwachung auf industriellem Niveau

Echelon und das Versagen des Europäischen Parlaments

von Heiner Busch

Echelon ist ein globales Abhörsystem, das vom US-Geheimdienst NSA dominiert wird. Von Juli 2000 bis Juli 2001 bemühte sich ein „nicht-ständiger Ausschuss" des Europäischen Parlaments (EP) um Aufklärung über dieses System und seine Wirkungen. Herausgekommen ist ein zwar durchaus lesenswerter, aber verheerend unpolitischer Bericht.[1]

Kann es ein weltumspannendes Überwachungssystem überhaupt geben? Wer könnte es mit welchen Mitteln betreiben? Welche Art und wessen Kommunikation wäre davon betroffen? Die Fragen, die sich der EP-Ausschuss stellte, bewegten sich nach wie vor im Konjunktiv.

Ein halbes Jahrhundert nach dem Geheimabkommen zwischen den USA, Großbritannien und den „Zweitparteien" (Kanada, Australien, Neuseeland), das die „SIGINT"-Allianz ihrer Geheimdienste begründete, ein Vierteljahrhundert, seitdem die Überwachung der satellitengestützten Kommunikation durch Echelon automatisiert wurde, trägt die öffentliche Diskussion hierüber immer noch Züge eines mittelalterlichen Gottesbeweises. Es gibt keine zusammenhängenden Regierungsberichte, wie sie die Parlamente normalerweise für ihre Kontrolltätigkeit benutzen; die wenigen öffentlich zugänglichen Informationen über Echelon wurden von spezialisierten Publizisten in jahrelanger mühevoller Kleinstarbeit zusammengetragen. Regierungsvertreter und hohe GeheimdienstlerInnen leugnen die Existenz des Überwachungssystems

1 Nicht-ständiger Ausschuss über das Abhörsystem Echelon: Bericht über die Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation v. 11.7.2001, www.europarl.eu.int/tempcom/echelon/pdf/rapport_echelon_de.pdf

nach wie vor, weshalb es keinen Sinn macht, sie zu befragen. Unmittelbar mit der Überwachung befasste Beamte unterliegen einer lebenslangen Schweigepflicht und wissen darüber hinaus meist nur das, was ihr unmittelbares Tätigkeitsfeld betrifft. Solche Leute haben ihr Wissen zwar Journalisten wie Nicky Hager und Duncan Campbell anvertraut; als Zeugen vor einem Parlamentsausschuss oder vor der Öffentlichkeit stehen allenfalls ausgestiegene GeheimdienstlerInnen zur Verfügung. Der Echelon-Ausschuss des EP war damit notwendigerweise auf „Indizien" angewiesen. Kritische Publizisten haben ihm dafür zwar die Fährten gezeigt, politisch ist der Ausschuss ihnen aber nicht gefolgt.

Satellitenkommunikation und Satellitenüberwachung

SIGINT – „signals intelligence" – bezeichnete anfänglich die Funküberwachung für militärische Zwecke. Die angloamerikanische Zusammenarbeit in diesem Bereich begann mit dem gemeinsamen Tracking von deutschen U-Booten und der Entschlüsselung des deutschen Flottencodes im Zweiten Weltkrieg. Sie blieb aber auch nach Kriegsende – genauer gesagt: im Kalten Krieg – erhalten und wurde 1947 durch das bereits zitierte, immer noch geheime Abkommen bekräftigt. Getragen wird diese „UKUSA"-Allianz (Vereinigtes Königreich, UK, und USA) von den technischen Geheimdiensten der USA (National Security Agency, NSA) und Großbritanniens (Government Communications Headquarters, GCHQ) sowie ihren Juniorpartnern in den drei Commonwealth-Staaten.

Im Zentrum steht dabei die Überwachung ziviler Telekommunikationssatelliten, die seit Mitte der 60er Jahre die alten Unterseekabel als vorherrschendes Transportmedium der transkontinentalen Telekommunikation ablösten. „Baut man eine Richtfunkstrecke zu einem stationär in großer Höhe stehenden Kommunikationssatelliten auf, der die Richtfunksignale empfängt, umsetzt und wieder zur Erde zurücksendet, so kann man ohne Einsatz von Kabeln große Entfernungen überbrücken. Die Reichweite einer solchen Verbindung ist nur dadurch beschränkt, dass der Satellit nicht um die Erdkugel herum empfangen und senden kann."[2] Der erste Satellit der International Telecommunications Satellite Organisation (Intelsat) wurde 1965 in seine Umlaufbahn gebracht, deckte aber nur die nördliche Hemisphäre ab. Die zweite und dritte Generation

2 ebd., S. 36

mit Positionen über dem Atlantik, dem Indischen und dem Pazifischen Ozean folgten 1967 und 1968 und erlaubten damit erstmals eine weltumspannende Kommunikation via Satellit. Die vierte Intelsat-Generation folgte ab 1971. Deren Überwachung begann im selben Jahr mit der Inbetriebnahme der Einrichtungen in Morwenstow (GB): Die Parabolantennen dieser Überwachungsstation sind auch heute noch auf die Satelliten über dem Atlantik und dem Indischen Ozean gerichtet; die großen Ohren in Yakima im Nordwesten der USA belauschten seit 1972/73 die Kommunikation über dem Pazifik. Mit der Ausweitung der Satellitenabdekkung erfolgte ab Ende der 70er Jahre auch eine Ausweitung des Netzes der Überwachungsstationen. Zehn Überwachungsstationen sah der EP-Bericht aufgrund der Antennenstellung und -größe eindeutig identifiziert, bei weiteren zehn, darunter Bad Aibling in Bayern, könne „die Funktion nicht eindeutig belegt werden."[3]

Vom Handbetrieb zum elektronischen Staubsauger

Noch bis in die 70er Jahre, so erklärt Duncan Campbell, habe man bei der NSA die Auswahl der wichtigen Elemente aus der Unmenge der abgefangenen Kommunikation mit Hilfe manueller Beobachtungslisten getroffen. Das Echelon-System, bereits Ende der 60er Jahre geplant und seit Ende der 70er betrieben, markiert den Beginn der Automatisierung. In einer Liste von Datenbanken, die 1979 in der Abhörstation Menwith Hill in Großbritannien benutzt wurden, findet sich u.a. „Echelon 2". „Zentrale Komponente des Systems sind lokale ‚Dictionary'-Computer, die eine umfangreiche Datenbank über spezifische Zielobjekte speichern – inklusive Namen, Themen von Interesse, Telefonnummern und andere Selektionskriterien. Eingehende Nachrichten werden mit diesen Kriterien verglichen; bei einem Treffer wird die ‚Roh-Intelligence' automatisch weitergeleitet."[4] Das Netzwerk, das die Aufklärungsstationen über Unterseekabel und militärische Satelliten mit den Verarbeitungszentren verbindet, ist das erste Wide Area Network der Welt gewesen. Erst Mitte der

3 ebd., S. 60

4 Campbell, D.: Interception Capablities 2000. Working document for the STOA Panel, Luxemburg 1999, p. 13, www.europarl.eu.int/stoa/publi/pdf/98-14-01-2_en.pdf

90er Jahre sei das öffentliche Internet größer als dieses „geheime Internet“ geworden.[5]

Vor dem EP-Ausschuss erklärte der neuseeländische Autor Nicky Hager, wie die Verteilung der Information und damit auch die Hierarchien unter den beteiligten Geheimdiensten funktionieren.[6] „Innerhalb der Allianz hat Neuseeland den Job, den südpazifischen Raum auszuspionieren. Die meisten Suchbegriffe im Echelon-System, die sich auf den Südpazifik beziehen, wurden von Neuseeland eingegeben. Die Nachrichten, die mithilfe dieser Begriffe abgefangen wurden, werden nach Wellington übermittelt, nicht nach Washington, denn es ist eine neuseeländische Liste von Suchwörtern.“ Sie würden von neuseeländischen Analysten ausgewertet, übersetzt und zu Berichten verarbeitet. Diese Berichte, nicht das Rohmaterial, würden weitergegeben an die NSA oder das GCHQ. „Aber in Waihopai wie in den anderen Stationen gibt es nicht nur die heimischen Suchwortlisten, sondern wohl separierte Listen amerikanischer, australischer, kanadischer oder britischer Überwachungsziele.“ Die meisten der von den Waihopai-Computern verwendeten Suchbegriffe stammen von den USA. Was aufgrund einer US-Liste abgefangen wird, „bekommt nie ein Neuseeländer zu Gesicht.“ Die rohen Daten gingen automatisch an die NSA und „die entscheiden, ob sie ihre Erkenntnisse später mit Neuseeland teilen wollen ... Da geht nicht alles in eine einzige große Datenbank, in der jeder nachsehen und finden kann, was er will. Die Amerikaner haben dieses System in einer sehr strukturierten und hierarchischen Weise angelegt.“

Ein unpolitischer Bericht

Für den Ausschuss war die zentrale Frage, ob mit Hilfe Echelons auch Wirtschaftsspionage betrieben werde. Entsprechende Vorwürfe waren in zwei im Auftrag der EP-Technikfolgenabschätzungseinheit (STOA) erstellten Berichten – darunter stammt einer aus der Feder von Duncan Campbell – erhoben worden. Dieser Verdacht bildete überhaupt erst den Anlass für die Einsetzung des Ausschusses. Campbell nannte zwei konkrete Beispiele, wo von der NSA abgehörte und weiter gegebene Infor-

5 Campbell, D.: Inside Echelon, in: Schulzki-Haddouti, C. (Hg): Vom Ende der Anonymität, Hannover 2000, S. 49-70 (53)

6 Hager, N.: Appearance before the EP Echelon Committee, http://cryptome.org/echelon-nh.htm, s.a. ders.: Secret Power, Wellington 1996

mationen dazu geführt hatten, europäische Unternehmen zugunsten von US-Unternehmen aus dem Rennen um Aufträge zu verdrängen: 1994 verlor die französische Thomson-CSF einen Auftrag in Brasilien an die Raytheon Corp., 1995 erhielt McDonnell Douglas in Saudi Arabien den Vorzug gegenüber Airbus. In beiden Fällen waren den europäischen Firmen Bestechungsversuche vorgeworfen worden. Diese Vorwürfe passten damit in die Rechtfertigung der US-Behörden, es gehe ihnen nicht um Wirtschaftsspionage, sondern um Korruptionsbekämpfung und um Verhinderung von Embargobrüchen. Campbells Vermutung, über das sog. „Advocacy Center" der US-Regierung würden von NSA und CIA erhobene Informationen an Wirtschaftsunternehmen weitergegeben, konnte der Ausschuss zwar nicht bestätigen, hielt sie aber, nachdem ihm ein Gespräch verweigert wurde, für wahrscheinlich. Nicky Hagers Argument, dass es im Zeitalter der Privatisierung und der transnationalen Unternehmen vor allem um wirtschafts- und handels*politische* Spionage gehe, etwa um die Überwachung von Delegationen bei GATT-Verhandlungen, hat der Ausschuss nicht mehr aufgegriffen.

Insgesamt bleibt der Bericht unpolitisch. Falls Konkurrenzspionage betrieben würde, verstoße dies gegen das Gemeinschaftsrecht. Insgesamt seien SIGINT-Aktivitäten, sofern sie sich auf den Schutz der nationalen Sicherheit bezögen, aber grundsätzlich von der Europäischen Menschenrechtskonvention gedeckt. Voraussetzung sei jedoch, dass sie – wie etwa die Aktivitäten des deutschen Bundesnachrichtendienstes – rechtlich fixiert und durch parlamentarische Gremien kontrolliert würden. Die politische Fragwürdigkeit der Spionage schlechthin – sei sie nun gegen (befreundete) Regierungen gerichtet oder gegen Nichtregierungsorganisationen (vom Roten Kreuz über Amnesty International bis hin zur Kampagne gegen Landminen) – fiel unter den Tisch. Das Telekommunikationsgeheimnis reduzierte der Ausschuss auf ein paar Datenschutzfloskeln und empfahl zum guten Schluss auch noch eine engere geheimdienstliche Kooperation der EU-Staaten.

Weder Echelon noch die „Staubsauger" anderer Staaten sind omnipotent. Spracherkennungsprogramme sind trotz großem finanziellen Aufwand gescheitert. Die interkontinentale Telekommunikation wird statt über Satelliten in wachsendem Maße über neue Glasfaser-Unterseekabel transportiert, die schwerer anzuzapfen sind. Das Problem der automatisierten Überwachung ist jedoch nicht erledigt. Die Arbeit an Schnittstellen für die Überwachung digitaler Telekommunikationssyste-

me läuft auf Hochtouren – und zwar unter Beteiligung der EU. Dass sie dann künftig auch im internationalen Rahmen von „gesetzlich ermächtigten Behörden“ betrieben werden soll, kann kaum beruhigen.

Die Cybercrime-Konvention[1]

Ein Schritt zum weltweiten Fahndungsnetz

von Sönke Hilbrans

Im Digitalzeitalter gibt es für Individuen wie für wettbewerbsorientierte Gesellschaften nur zwei stabile Zustände: online oder tot. Entsprechend erscheint der Politik der inneren Sicherheit die Sicherheit „im Netz" als vorrangige Aufgabe moderner Daseinsfürsorge. Wegen der steigenden wirtschaftlichen und politischen Bedeutung der Netze sieht der „libertäre oder anarchistische Traum vom Internet"[2] einem Erwachen im Netz polizeilicher Zugriffe entgegen.

Nach langer Diskussion[3] haben sich die 43 Mitgliedstaaten des Europarates unter Mitwirkung von Kanada, den USA, Japan und der Republik Südafrika auf die Cybercrime Convention (CCC)[4] verständigt. Die Konvention soll ermöglichen, dass Straftaten, die in oder unter Zuhilfenahme von Telekommunikations- oder Datennetzen begangen werden, zukünftig effektiver und international bekämpft werden können. Der am 23.11.2001 in Budapest unterzeichnete Text bestätigt die Befürchtungen der Fachwelt: die CCC zielt auf die Ausstattung der Polizeien der Signatarstaaten

1 überarbeitete und gekürzte Fassung des Beitrages „Verfassungskonflikte im Cyberspace", in: Datenschutz-Nachrichten (DANA) 2001, H. 2, S. 16-21

2 Berichterstatter Tallo der Parlamentarischen Versammlung des Europarates in der Debatte vom 24.4.2001 zum 25. CCC-Entwurf, www.cyber-rights.org/documents/coe_assembly.htm.

3 s. zur Vorgeschichte: Kugelmann, D.: Die „Cyber-Crime" Konvention des Europarates, in: Datenschutz und Datensicherheit (DuD) 2001, H. 4. S. 215-223

4 Convention on Cybercrime, ETS No. 185, http://conventions.coe.int/treaty/en/treaties/html/185.htm)

mit weitreichenden Eingriffsbefugnissen, ohne Gegengewichte im Sinne der Grundrechte zu schaffen.

Materielles Strafrecht

Die 48 Artikel der Konvention enthalten Vorgaben für drei Bereiche: für das Strafrecht und das Strafprozessrecht der Nationalstaaten sowie für die internationale juristische und polizeiliche Kooperation in Delikten des „Cybercrime".

In den Art. 2-11 macht die Konvention den Signatarstaaten Vorgaben über die „Cyber"-Straftaten, die sie in ihr Strafrecht aufnehmen müssen. Der Katalog reicht von illegalem Eindringen in Computernetze über das Stehlen oder Manipulieren von Daten bis zu einer Reihe von Delikten, die unter Zuhilfenahme von Datennetzen verübt werden können. Darüber hinaus verpflichten sich die Staaten, auch andere Straftaten, die mit Hilfe von Computersystemen begangen werden, unter Strafe zu stellen (Art. 14 CCC). Wohl alle im Umlauf befindlichen Fallbeispiele für „Cybercrime" – Anbahnung von Geschäften mit Bannware, Verbreitung strafbarer Inhalte im Internet, Betrug, Urheberrechtsverstöße, diverse Formen von „Angriffen" auf Computersysteme – werden bereits vom geltenden deutschen Strafrecht erfasst. Insgesamt betrifft die Konvention keineswegs besonders schwere oder gefährliche Straftaten; in strafrechtlicher Hinsicht liegt ihre Bedeutung vielmehr darin, dass sie ein international einheitliches Niveau festschreibt, das die Grundlage für vereinfachte Formen internationaler Strafverfolgung bilden soll.

Um strafbare Handlungen oder vorbereitende bzw. unterstützende Kommunikationsvorgänge sichtbar zu machen, bedürfte es idealerweise einer Kopie aller in Frage kommenden Daten zu jedem in Frage kommenden Zeitpunkt. Das klingt monströser, als es von der derzeitigen Praxis entfernt ist, denn viele der in Datennetzen kommunizierten und produzierten Informationen – insbesondere Verbindungs- und Bestandsdaten – bleiben auch ohne sicherheitsbehördliche Bedarfsanmeldung länger erhalten, als zur Abwicklung der Kommunikation erforderlich wäre. Den Zugang zu diesen Informationen durch Anpassung der technischen Rahmenbedingungen und rechtlichen Schnittstellen sicherzustellen, ist das zentrale Projekt der CCC.

Ermittlungsmethoden neuen Typs

Dazu wird ein internationaler Mindestbestand formuliert: Zugriff der nationalen Sicherheitsbehörden auf in Computern gespeicherte Informationen, den Inhalt von Telekommunikation sowie auf Bestands- und Verbindungsdaten. Soweit sich Daten auf einem Übertragungsweg befinden, sollen sich die Mitgliedstaaten, ggf. unter Zuhilfenahme der Provider, in die Lage versetzen, Verbindungs- wie Inhaltsdaten von Kommunikationsvorgängen in Echtzeit durch ihre Sicherheitsbehörden zur Kenntnis nehmen zu können. Welche Kommunikationsvorgänge derart überwacht werden können, bleibt den nationalen Regelungen überlassen (Art. 16, 18-21 CCC).

Eine erste Reaktion der deutschen Gesetzgebung setzte daher auch nicht im materiellen Strafrecht an, sondern – offenbar in Anlehnung an Art. 14 CCC – im Strafverfahrensrecht: Nach dem neuen § 100g Abs. 1 S. 1 der Strafprozessordnung (StPO) können in Zukunft (bestimmte) Verbindungsdaten schon dann erhoben werden, wenn jemand eine Straftat mittels einer Telekommunikationsendeinrichtung (§ 3 Nr. 3 Telekommunikations-Gesetz, TKG) begangen hat. Der schnelle Zugang zu Verbindungs- und Inhaltsdaten ist durch die Telekommunikationsüberwachungs-Verordnung (TKÜV) vom 22.1.2002 schon weitgehend vorweggenommen – auch wenn noch weiterer Anpassungsbedarf besteht.

Internationalisierung der Strafverfolgung

Neben der Standardisierung der Telekommunikationsüberwachung auf hohem Niveau zielt die CCC auf die internationale Verfügbarkeit der zu gewinnenden Erkenntnisse. Das Instrumentarium ist aus der polizeilichen Kooperation innerhalb der EU (Schengen, Europol) bekannt: die Zulassung von Spontanübermittlungen, jederzeit erreichbare Zentralstellen und die Vereinfachung der Kommunikationsprozesse zwischen den beteiligten Behörden (Art. 25, 27 und 35 CCC).

Ein neues Werkzeug sind „freeze-orders“: Auf qualifizierte Anfrage eines Signatarstaates soll ein anderer Staat in seinem Territorium vorliegende Verbindungs- und Inhaltsdaten bis zu 60 Tagen vorläufig sichern und ggf. Hinweise auf Provider in anderen Staaten weitergeben. Die so zu konservierenden Daten werden im Rahmen der internationalen Rechtshilfe übermittelt. Verbindungsdaten sollen nach Maßgabe des nationalen Rechts jedenfalls dann übermittelt werden, wenn sie bei inländischem Sachverhalt den Sicherheitsbehörden zur Verfügung stünden. Die besonders sensiblen Inhaltsdaten werden nach Maßgabe des jeweils Anwen-

dung findenden nationalen und internationalen Rechts übermittelt, ohne dass die CCC dazu eine eigene Aussage trifft (Art. 29-33 CCC).
Erfolgt die vorläufige Sicherung von gespeicherten Daten auf Anfrage eines Signatarstaates, stehen diesem mindestens 60 Tage zur Formulierung eines Rechtshilfeersuchens zur Verfügung. Abzuwarten bleibt, inwieweit der deutsche Gesetzgeber dieser Regel Rechnung tragen wird, da der Zugriff auch auf Verbindungsdaten bisher einem Richtervorbehalt unterliegt (§ 100h Abs. 2 StPO), der allenfalls für drei Tage durch eine staatsanwaltschaftliche Eilanordnung ersetzt werden kann (§ 100b Abs. 1 StPO). Eine sorgfältige Aufarbeitung des Erkenntnismaterials aus den die Datensicherung verlangenden Signatarstaaten dürfte in der Praxis zu erheblichen Schwierigkeiten führen, wenn nicht die Gerichte zukünftig auf bloßen Zuruf Beschlüsse nach § 100g StPO erlassen wollen.

Cyberspace ohne Privatheit?

Wo ein virtueller rechtsfreier Raum nicht existieren darf, sind es vor allem die informationelle Selbstbestimmung und das Telekommunikationsgeheimnis – international anerkannt durch das Recht auf Privatsphäre (Art. 8 Abs. 1 der Europäischen Menschenrechtskonvention) – denen im Kampf um die Durchsetzung der Rechtsordnung im „cyberspace“ Opfer abverlangt werden.

Denn die Besonderheiten der Datennetze potenzieren nicht die Verwundbarkeit der öffentlichen Sicherheitsinteressen, sondern der Grundrechte: Die Speicherung von Verbindungsdaten ergibt informationelle Bewegungsprofile der Betroffenen; sie hat damit einen Informationswert vergleichbar einer flächendeckenden Videoüberwachung im Cyberspace. Bestandsdaten im Telekommunikationsverkehr sind erheblich umfangreicher als die „Bestandsdaten“ des postalischen Briefverkehrs (vgl. Art. 18 Abs. 1 CCC oder, (noch) enger gefasst: §§ 89 Abs. 6, 90 Abs. 1 TKG). Kaum ein anderes privates Vertragsverhältnis des alltäglichen Lebens ist so gut dokumentiert und schon nach der TKÜV so weitgehenden Offenbarungspflichten ausgesetzt wie ein Telefon- oder Internet-Servicevertrag. Das Internet in den Händen der Sicherheitsbehörden wird zum Fahndungsnetz. Die CCC ist ein Meilenstein zur internationalen Harmonisierung und Forcierung dieser Entwicklung.

Die CCC enthält sich – trotz energischer Kritik der Fachöffentlichkeit, Datenschutzbeauftragten und auch aus der EU-Kommission – auch nach einigen Nachbesserungen hinreichend tragfähiger Aussagen zum Schutz

der Privatsphäre bzw. des Telekommunikationsgeheimnisses. Die von den beteiligten Behörden zu beachtenden Standards sind veraltet und kaum geeignet, der internationalen Kooperation der Sicherheitsbehörden effektive Schranken im Interesse der BürgerInnenrechte zu setzen. Zwar wird der Anschluss an die vorgefundene (datenschutz-)rechtliche Umgebung in Europa hergestellt. Diese verdichtet aber das vertragliche Schutzprogramm für die Grundrechte nicht zu einem inhaltlich tragfähigen Standard. Soweit Nicht-Mitgliedstaaten des Europarates der CCC beitreten (USA, Kanada, Japan, Südafrika), fehlt es ohnehin an einer vertraglichen Bindung. Der Grundrechtsschutz bleibt mit diesen Vorgaben Aufgabe der nationalen Rechtsordnungen (Art. 15 CCC), denen die Beachtung völkerrechtlicher Menschenrechtsgarantien und das Prinzip der Verhältnismäßigkeit anempfohlen ist. In der Bundesrepublik wird dadurch kein Änderungsbedarf ausgelöst.

Im Hinblick auf das Niveau des Datenschutzes erlaubt die Konvention den Signatarstaaten große Spielräume. So soll die Erhebung von Inhaltsdaten an einen Katalog schwerer Straftaten gebunden werden. Auch für die Erhebung von Verbindungsdaten besteht die nationale Option für derartige Kataloge. Die Computerüberwachung in Echtzeit (nach Art. 20 und 21 CCC) soll nur nach Maßgabe des nationalen Rechts bestimmte („spezifizierte“) Kommunikationen betreffen – über Mindestspezifikationen als Abgrenzung zur anlasslosen Totalerfassung schweigt sich der Text aus, obgleich das Problem erkannt wurde. Entsprechend wird sich auch der deutsche Gesetzgeber nicht zu einer Reaktion veranlasst sehen.

Aus dem datenschutzrechtlichen Gefälle zwischen den Signatarstaaten müsste folgen, dass Unterschiede im Schutzniveau zur Verweigerung der Rechtshilfe berechtigen müssen. Die CCC folgt dieser Konsequenz bewusst nicht. Ebenso findet sich kein Wort zu grenzüberschreitenden Rechten und Ansprüchen der Betroffenen. Ob, wie und nach welchem Verfahren Auskunft oder Mitteilung über die Übermittlung personenbezogener Daten zu machen ist, bleibt Sache des nationalen Rechts, obwohl gerade in diesen Fragen erhebliche Unterschiede zwischen den beteiligten Rechtsordnungen bestehen – und unangetastet bleiben.

Sönke Hilbrans ist Rechtsanwalt in Berlin und Mitglied im Vorstand der Deutschen Vereinigung für Datenschutz (DVD).

„Etwas von Folter ..."

Tödlicher Brechmitteleinsatz in Hamburg

von Fredrik Roggan

Dass der Eindruck habe entstehen können, beim Einsatz von Brechmitteln handele es sich um eine „alltäglich anzuwendende abschreckende Strafe statt um notwendige Beweissicherung", das ertrage er nicht. So begründete der Leiter des Hamburger Landeskriminalamtes am 16. Januar 2002 das Rücktrittsgesuch an seinen Vorgesetzten. Wenige Tage zuvor war ein 19-jähriger Kameruner an den Folgen eines solchen Brechmitteleinsatzes gestorben.[1]

Achidi J. war am 9. Dezember 2001 unter dem Verdacht des Drogenhandels festgenommen und ins Rechtsmedizinische Institut des Hamburger Universitätskrankenhauses Eppendorf gebracht worden. Da die Polizei davon ausging, dass er die Drogenportionen verschluckt hatte, wurde der Einsatz des Brechmittelsirups Ipecacuanha angeordnet. Achidi J. warnte, dass er sterben werde. Dennoch hielten vier Polizisten den sich heftig wehrenden Mann fest, während eine Ärztin ihm – nach zwei vergeblichen Versuchen – insgesamt 30 Milliliter Brechmittelsirup und 800 Milliliter Wasser durch eine Magensonde einflößte. Danach war der junge Mann zu Boden gerutscht und regungslos liegen geblieben. Nach dreitägigem Koma war er am 12. Dezember 2001 verstorben.[2]

Der Hamburger Todesfall hat eine längere Vorgeschichte. Immer wieder war von Betroffenen zu hören, dass sie nach einer solchen Brachialbehandlung tagelang Beschwerden wie Brechanfälle, Durchfall, Ap-

1 Die Welt (Hamburg) v. 8.2.2002

2 vgl. etwa Frankfurter Rundschau v. 11.12.2001

petitlosigkeit und Herzbeschwerden hatten.[3] Mitunter mussten sich Betroffene anschließend für mehrere Tage in stationäre Behandlung begeben.[4] In Bremen erlitt 1996 ein 16-Jähriger nach der Brechprozedur einen Schwächeanfall, so dass ein Rettungswagen kommen musste. Ein Bremer Hausarzt hat mehrfach erlebt, dass mit dem Brechmittel Ipecacuanha traktierte Patienten körperlich und seelisch traumatisiert waren. In einem Fall registrierte er Erosionen der Magenschleimhaut und blutiges Erbrechen über mehrere Tage.[5] Schon diese bekannt gewordenen Einzelfälle – das Dunkelfeld ist unbekannt – widerlegen die gelegentlich aufgestellte Behauptung, der zwangsweise Einsatz solcher Vomitiv-mittel sei „harmlos“[6] oder – wie z.B. zwangsweise Blutprobenentnahmen – „absolut ungefährlich“.[7]

1997 fällte das Oberlandesgericht Frankfurt ein Grundsatzurteil zum zwangsweisen Brechmitteleinsatz: In einem Fall, in dem der Betroffene nach einer solchen Behandlung bewegungsunfähig war und auf einem Aktenbock in die Haftzelle gefahren werden musste, entschied das Gericht, dass eine solche Behandlung unter keinem rechtlichen Gesichtspunkt zulässig sei. Die Beweismittel waren also rechtswidrig erlangt worden. Sie durften nicht verwertet und der Betroffene musste freigesprochen werden.[8] Für die Generalstaatsanwaltschaften von Berlin und Hessen war jenes Urteil der Anlass gewesen, die Brechmittelanwendung – vorübergehend – auszusetzen.

Das Wissen des Hamburger Justizsenators

Maßstab für die Zulässigkeit des Brechmitteleinsatzes ist § 81a der Strafprozessordnung (StPO). Dort heißt es in Absatz 1 Satz 2, dass körperliche Eingriffe ohne Einwilligung des Beschuldigten nur dann zulässig sind,

3 Dettmeyer, R.; Musshoff, F.; Madea, B.: Die zwangsweise Verabreichung von Vomitivmitteln als ärztlicher Eingriff gem. § 81a I StPO, in: Medizinrecht 2000, H. 7, S. 319

4 vgl. dazu die Gesprächsprotokolle in der Broschüre des Antirassismusbüros Bremen: „Polizisten, die zum Brechen reizen“, Bremen 1995, S. 21 ff.

5 Frankfurter Rundschau v. 18.12.2001

6 Birkholz, M.; Kropp, St.; Bleich, St. u.a.: Exkorporation von Betäubungsmitteln, in: Kriminalistik 1997, H. 4, S. 282

7 so z.B. Kleinknecht, Th.; Meyer-Goßner, L.: Strafprozeßordnung, München 2001, § 81a Rdnr. 13

8 OLG Frankfurt, Neue Juristische Wochenschrift 1997, H. 24, S. 1647-1649; Weßlau, E.: Anmerkung zu OLG Frankfurt, in: Strafverteidiger 1997, H. 7, S. 341-344

wenn kein Nachteil für seine Gesundheit zu befürchten ist. Gesundheitliche Nachteile müssen also mit an Sicherheit grenzender Wahrscheinlichkeit auszuschließen sein.[9]

In der medizinischen Literatur wird aber nicht nur vor den Risiken des im konkreten Fall eingesetzten Brechsirups Ipecacuanha gewarnt, der starke Bewusstseinstrübungen und manifeste Herz- und Ateminsuffizienz auslösen könne.[10] Vielmehr muss der Einsatz von Brechmitteln grundsätzlich in Frage gestellt werden. Die Gefahren eines solchen Eingriffs waren auch Hamburgs Justizsenator Roger Kusch nicht unbekannt. Einen Tag vor dem Tod des jungen Kameruners beschrieb Kusch in einem Zeitungsinterview, dass es am Kehlkopf Nerven gebe, die bei Berührung – etwa durch eine Magensonde – einen Herzstillstand auslösen könnten.[11] Hierbei handelt es sich um den Nervus vagus (Vagus-Nerv), der Teil des parasympathischen Nervensystems ist. Im Gegensatz zum Sympathikus, der für die Zunahme der Herzfunktionen – zum Beispiel zur Bewältigung von Flucht- und Angriffssituationen – verantwortlich ist, sorgt der Nervus vagus nach Reizung für die Abnahme von Herzfrequenz und Kontraktionskraft des Herzmuskels.[12] Beim zwangsweisen Einführen einer Magensonde gegen den Widerstand des Betroffenen oder auch beim Vorgang des Brechens an sich besteht demnach das Risiko, dass dem menschlichen Organismus ein Impuls vermittelt wird, der der natürlichen Abwehrreaktion des sympathischen Nervensystems widerspricht. Das mit diesem Impuls verbundene Risiko reicht bis zum Stillstand des Herzens. Wie stark der Nervus vagus reagiert, lässt sich – auch bei vorheriger ärztlicher Untersuchung – nicht exakt vorhersehen. Maßgeblich sind sowohl die momentane wie auch generelle körperliche Konstitution des Betroffenen, die Tageszeit etc.

Weiterhin besteht bei jedem Einführen einer Magensonde die Gefahr, dass der Schlauch in der Lunge statt im Magen landet und dadurch schwerste innere Verletzungen hervorruft oder dass der Erbrechende Teile des Erbrochenen aspiriert, d.h. in die Lunge einatmet.[13] Nach Ein-

9 vgl. nur Kleinknecht, Th.; Meyer-Goßner, L. a.a.O. (Fn. 7), § 81a Rdnr. 17

10 Dettmeyer, R.; Musshoff, F.; Madea, B. a.a.O. (Fn. 3), S. 319

11 Hamburger Abendblatt v. 11.12.2001

12 vgl. dazu etwa Jänig, W.: Vegetatives Nervensystem, in: Schmidt, R.; Thews, G. (Hg.): Physiologie des Menschen, Berlin 1995, S. 340–343

13 Dallmeyer, J.: Verletzt der zwangsweise Brechmitteleinsatz gegen Beschuldigte deren Persönlichkeitsrechte?, in: Strafverteidiger 1997, H. 11, S. 606-610 (607)

schätzung der Hamburger Ärztekammer liegen in der gewaltsamen Verabreichung von Brechmitteln so viele Risiken, „dass man das nicht machen darf".[14] Von einer an Sicherheit grenzenden Wahrscheinlichkeit, dass die zwangsweise Brechmittelanwendung gesundheitlich unbedenklich sei, kann also ganz und gar nicht ausgegangen werden.

Die Reaktionen der Politik auf den Todesfall

Schon kurze Zeit nach dem Tod von Archidi J. wurden in Hamburg wieder Brechmitteleinsätze angeordnet.[15] Auch ansonsten schien man recht unbeeindruckt: Der „tragische Zwischenfall", so Justizsenator Kusch, sei der Preis, den die „politische Arbeit" verlange. Das Todesrisiko bei solch einer gewaltsamen Prozedur sei „allen im vollen Umfang bewusst" gewesen.[16] An der gewaltsamen Brechmittelanwendung solle aber dennoch festgehalten werden, denn: „Eine Änderung der Praxis wäre ein Signal, dass die Strafverfolgung in Hamburg nicht mit der gebotenen Härte durchgeführt wird".[17] Auch Innensenator Ronald Barnabas Schill lehnte die Beendigung des Brechmitteleinsatzes ab. Dies sei ein „falsches Signal an Kriminelle".[18] Beide bestätigten damit den Verdacht des zurückgetretenen LKA-Chefs, dass der Brechmitteleinsatz eine „abschreckende (Quasi-)Strafe" sei.

Indessen: Die Hamburger Drogenpolitik bewegt sich mit der planmäßigen Brechmittelverabreichung auf juristisch brüchigem Eis. Sie bedeutet nämlich eine Instrumentalisierung von lediglich Verdächtigen einer Straftat, die mit der Aufgabe des Strafverfahrens nicht in Einklang zu bringen ist: Ziel dieser Methode ist Abschreckung. Am lediglich verdächtigen Individuum soll verdeutlicht werden, dass bestimmte Störungen der öffentlichen Sicherheit nicht toleriert würden. Abschreckung hat im Ermittlungsverfahren aber nichts verloren. Verdächtige haben bis zu ihrer rechtskräftigen Verurteilung als unschuldig zu gelten. Ihnen dürfen nur solche Beschränkungen auferlegt werden, die zur Sicherung des (Straf-)Verfahrens erforderlich sind. Eine vorweggenommene Quasi-Sanktionierung ist kategorisch unzulässig, weil sie die Betroffenen zum

14 zit. n. Frankfurter Rundschau v. 11.12.2001
15 Die Welt (Hamburg) v. 28.12.2001
16 zit. n. Hamburger Abendblatt v. 11.12.2001
17 zit. n. Frankfurter Rundschau v. 11.12.2001
18 zit. n. Weser-Kurier v. 12.12.2001

Objekt degradiert. Eine verfassungsrechtliche Rechtfertigung für eine auch aus Gründen der Abschreckung vollstreckbare staatliche Maßnahme (Bsp.: Freiheitsstrafe) kann es ausschließlich bei rechtskräftigen Verurteilungen geben.[19] Das Verbot von Verdachtsstrafen muss im Rechtsstaat uneingeschränkt gelten; generalpräventive Zwecke dürfen allenfalls durch ein rechtskräftiges Urteil bewirkt werden.[20] Davon aber kann in Hamburg offensichtlich nicht mehr ausgegangen werden.

Alternativen zur Brechmitteltortur

Es bleibt die Frage, weshalb angesichts der nach dem Todesfall offenkundigen Risiken von der Brechmittel-Methode überhaupt Gebrauch gemacht wird, denn es gibt Alternativen. Der Zoll in Hamburg, der wie die Polizei im Bereich der Drogenfahndung tätig ist, wartet bei entsprechendem Verdacht das Ausscheiden der verschluckten Drogenpäckchen auf natürlichem Wege ab.[21] Ebenso verfährt Hamburgs Nachbarland Niedersachsen. Abgelehnt wird die Vorgehensweise der Hamburger Polizei deswegen, weil die zwangsweise Verabreichung von Ipecacuanha als „lebensgefährlich“ eingestuft wird.[22]

Bei der Anwendung der Brechmittel-Methode scheint es sich jedoch um eine kriminalpolitische Grundsatzentscheidung zu handeln, die – wie gezeigt – nur „unter anderem“ mit Zwecken der Strafverfolgung gerechtfertigt wird. Diese Entscheidung war unter dem rot-grünen (Vorgänger-)Senat zunächst noch anders ausgefallen: In einer gemeinsamen Presseerklärung von Innen- und Justizbehörde vom 7. Februar 2001 hatte es ausdrücklich geheißen: „Die Verabreichung von Brechmitteln als eine Art der ‚Sofortstrafe‘ wird abgelehnt“.[23] Bereits die Kandidatur des als „Richter Gnadenlos“ bekannten heutigen Innensenators hatte ausgereicht, um die SPD-GAL-Regierung von ihrer Linie abzubringen. Wohl um kriminalpolitische Entschlossenheit zu demonstrieren, kippte der Senat am 5. Juli 2001 seine Entscheidung vom Februar. Nunmehr wur-

19 Roggan, F.: Generalprävention bei polizeirechtlichen Entscheidungen?, in: Kritische Justiz 1999, H. 1, S. 74

20 ausführlich dazu Frister, H.: Verbot der Verdachtsstrafe und Unschuldsvermutung als materielle Grundprinzipien des Strafverfahrens, Berlin 1988, S. 93

21 Pötzl, N.: Abgang via naturalis, in: Spiegel Nr. 51/2001, S. 32 f.

22 so der dortige Justizminister Pfeiffer, siehe Frankfurter Rundschau v. 18.12.2001

23 www.hamburg.de/Behoerden/Pressestelle/Meldungen/tagesmeldungen/2001/feb/w06/mi/news.htm

den mit rot-grünem Segen Brechmittel gegen (mutmaßliche) Kleindealer eingesetzt.[24]

Das schlechte Gewissen des Bundesverfassungsgerichts

Nach der Hamburger Tragödie war ein wahrlich ungewöhnlicher Vorgang zu registrieren: Das Bundesverfassungsgericht (BVerfG) wandte sich mit dem Anliegen an die Öffentlichkeit, ein scheinbar bestehendes Missverständnis aus der Welt zu schaffen. Die Pressesprecherin der Karlsruher RichterInnen schrieb in einer auf der Leserbriefseite (!) der Berliner Zeitung veröffentlichten Erklärung: Es sei nicht richtig, dass das Bundesverfassungsgericht bereits über die Vereinbarkeit der Brechmittelverabreichung mit dem Grundgesetz entschieden habe. Zu diesem Thema existiere lediglich ein Kammerbeschluss.[25] Mit diesem Beschluss sei eine Verfassungsbeschwerde aus prozessualen Gründen nicht angenommen worden. Eine Auskunft über die Verfassungsmäßigkeit dieses Vorgehens gebe der Beschluss aber nicht.[26]

Die Ursache für diese „Einmischung" in die Tagespolitik dürfte darin liegen, dass die Generalstaatsanwaltschaften von Hessen und Berlin gestützt auf eben diesen Beschluss die zwischenzeitlich der Polizei untersagte Brechmittelanwendung wieder zugelassen hatten. Auch das Kammergericht Berlin berief sich unmittelbar auf die nur vermeintlich unmissverständliche Karlsruher Rechtsprechung. Auf die in Rechtsprechung und Literatur geäußerten (verfassungsrechtlichen) Bedenken gegen diese Art der Beweismittelgewinnung ging es gar nicht erst ein.[27]

Folter zur Sicherung von Beweismitteln?

Zusammenfassend ist zu konstatieren, dass der zwangsweise Brechmitteleinsatz zur Erlangung von Beweismitteln in Form von verschluckten Drogenportionen in vielerlei Hinsicht rechtswidrig ist: Die Voraussetzun-

---

24 Berliner Zeitung v. 12.12.2001

25 BVerfG, Strafverteidiger 2000, H. 1, S. 1-3 (mit kritischer Anmerkung von W. Naucke); Rixen, St.: Anmerkung zu BVerfG, in: Neue Zeitschrift für Strafrecht 2000, H. 7, S. 381f. und Rachor, F.: Polizeihandeln, in: Lisken, H.; Denninger, E (Hg.): Handbuch des Polizeirechts, München 2001, S. 471

26 Berliner Zeitung v. 15.12.2001, BVerfG-Pressemitteilung Nr. 116 v. 13.12.2001

27 Kammergericht Berlin, Juristische Rundschau 2001, H. 4, S. 162 (insbes. S. 163); vgl. auch OLG Bremen, Neue Zeitschrift für Strafrecht 2000, H. 9, S. 270

gen des § 81a Absatz 1 StPO liegen nicht vor. Weder kann festgestellt werden, dass eine Beeinträchtigung des körperlichen Wohlbefindens über die Untersuchungsdauer hinaus ausgeschlossen ist. Schon gar nicht kann mit an Sicherheit grenzender Wahrscheinlichkeit angenommen werden, dass der Brechmitteleinsatz gesundheitlich unbedenklich sei – insbesondere dann nicht, wenn das Mittel mithilfe einer Magensonde gewaltsam eingeflößt wird. In Betracht käme die Verabreichung eines Brechmittels allenfalls dann, wenn es tatsächlich freiwillig geschluckt würde. Weigert sich der Betroffene, so ist der Brechmitteleinsatz ausnahmslos unzulässig.

„Beweismittel unter Qualen aus einem Körper zu holen, hat etwas von Folter", sagt Bernd Kalvelage von der Hamburger Ärzteopposition.[28] Und mit einer solchen rechtsethischen Bewertung liegt der Mediziner vermutlich noch ein wenig näher am Kern der hier behandelten Problematik als die zitierten juristischen Ausführungen.

Fredrik Roggan ist Mitglied des Bundesvorstandes der Humanistischen Union und Autor des Buches „Auf legalem Weg in einen Polizeistaat", Bonn 2000 (Pahl-Rugenstein).

28 zit. n. Die Woche v. 14.12.2001

Terrorismusbekämpfungsgesetz in Kraft

Der Ausbau der Sicherheitsapparate geht voran

von Norbert Pütter

Lediglich sechs Wochen benötigte der Bundesgesetzgeber, um das „Gesetz zur Bekämpfung des internationalen Terrorismus“[1] in Kraft zu setzen. In 22 Artikeln verschärft das Gesetz eine Reihe von rechtlichen Bestimmungen, die von A wie „Ausländerrecht“ bis Z wie „Zentralregister“ reichen. Ob die neuen Kontroll- und Erfassungsbefugnisse tatsächlich der „Bekämpfung“ des Terrorismus dienen, steht in den Sternen. Sicher ist in jedem Fall, dass sie das Überwachungspotential der Sicherheitsapparate stärken.

Die nachhaltigen Veränderungen im Bereich des Ausländer- und Asylrechts haben wir bereits in der letzten Ausgabe dargestellt.[2] Sie betreffen insbesondere die Ausweitung der Versagungsgründe bei der Visaerteilung, die Beteiligung der Nachrichtendienste, des Zollkriminalamtes und des Bundeskriminalamtes am Visumverfahren, die Verschlechterung des Rechtsschutzes gegen Ausweisungen, die Aufnahme biometrischer Merkmale in die Aufenthaltsgenehmigung und den Ausweisersatz, die Anfertigung von Sprachaufzeichnungen im Asylverfahren, die Angabe der Religionszugehörigkeit im Ausländerzentralregister etc.

Zwei Bestimmungen gehen deutlich über die als Terrorismusbekämpfung getarnte Migrationskontrolle hinaus: Zum einen werden das „Bundesamt für die Anerkennung ausländischer Flüchtlinge“ und die

1 Bundesgesetzblatt Teil I, Nr. 3 v. 11.1.2001, S. 361-395. Zum Gesetzgebungsverfahren und zur Kritik am Gesetz s. www.cilip.de/terror

2 Lederer, A.: Sicherheitsrisiko Nr. 1, in: Bürgerrechte & Polizei/CILIP 70 (3/2001), S. 35-41

Ausländerbehörden der Länder verpflichtet, die „die ihnen bekannt gewordenen Informationen einschließlich personenbezogener Daten“ an die Ämter für Verfassungsschutz zu übermitteln, sofern sie vermuten, dass diese Daten für die Ämter erforderlich sind. Mit dieser Bestimmung werden die Ausländerbehörden zu flächendeckenden Sammelstellen der deutschen Inlandsgeheimdienste.

Für die Polizeien hingegen ist der novellierte Paragraf 16 des Asylverfahrensgesetzes von großer praktischer Bedeutung. Die neue Regelung erweitert die gespeicherten erkennungsdienstlichen Daten um Sprachaufzeichnungen der Asylsuchenden. Diese Unterlagen, die 10 Jahre aufbewahrt werden müssen, können genutzt werden „zur Feststellung der Identität oder Zuordnung von Beweismitteln für Zwecke des Strafverfahrens oder zur Gefahrenabwehr“. Selbstverständlich ist auch hier nicht von terroristischen Gefahren oder Straftaten die Rede. Vielmehr werden alle Flüchtlinge in Deutschland erfasst; und ihre Daten stehen von nun an für jede Art polizeilicher Arbeit zur Verfügung.

Geheimdienste im Aufwind

Der Aktionismus des Gesetzgebers hat den drei Geheimdiensten neue Quellen und Tätigkeitsbereiche erschlossen. Das Bundesamt für Verfassungsschutz wird ermächtigt, bei Unternehmen der Finanz- und Kreditwirtschaft, von Postdienstleistern, Luftfahrunternehmen und Telekommunikationsanbietern Informationen über Kunden bzw. Nutzer einzuholen. Dem Bundesnachrichtendienst wird Zugang zu Finanzinstituten und zu den Telekommunikationsdiensten eröffnet. Damit erhält der Auslandsgeheimdienst eine weitere Ausforschungskompetenz im Innern. Auch der Militärische Abschirmdienst (MAD) darf nun Auskunft von den Telekommunikationsanbietern verlangen. Da der MAD sich für alle Personen interessieren kann, die zukünftig in der Bundeswehr tätig sein sollen, geraten alle potentiell Wehrpflichtigen in sein Visier. Zwar enthält das Gesetz keine Verpflichtung für die Unternehmen, die gewünschten Daten zu liefern, aber bis diese Regelungen geschaffen sind, wird sich wohl kein Unternehmen dem vermeintlichen „Kampf gegen den Terrorismus“ widersetzen wollen.

Die Änderung des „Sicherheitsüberprüfungsgesetzes“ verschafft den Verfassungsschutzbehörden ein zusätzliches Betätigungsfeld. Die Überprüfung durch die Dienste erstreckt sich nun auch auf Beschäftigte, die in „lebens- oder verteidigungswichtigen“ Einrichtungen arbeiten. Welche

Einrichtungen dies sind, wird die Bundesregierung in einer Verordnung festlegen. Offenkundig ist, dass mit dieser Bestimmung die ArbeitnehmerInnen in den Infrastrukturbereichen Wasser, Energie, Telefon und Verkehr Kandidaten für Sicherheitsüberprüfungen und damit Objekte nachrichtendienstlichen Interesses sein werden.

Bundespolizeiliche Terraingewinne

Verglichen mit den Nachrichtendiensten ist der „Gewinn" für die Polizeien bescheidener. Für den Bundesgrenzschutz (BGS) wird der Grenzstreifen, in dem er „verdachtsunabhängig" kontrollieren darf, an den Seegrenzen von 30 auf 50 Kilometer erweitert. Durch Rechtsverordnung kann dieser Streifen auf maximal 80 Kilometer erweitert werden. Kontrollierte Personen müssen mitgeführte Ausweispapiere „zur Prüfung" aushändigen. Da Deutsche nicht verpflichtet sind, Ausweise mitzuführen, trifft diese Befugnis wiederum besonders Ausländer. Die Ausweitung des „Grenzstreifens" umfasst zudem größere Städte von Wilhelmshaven bis Rostock. Damit entwickelt sich der BGS weiter zu einer im gesamten Bundesgebiet zuständigen Polizei; durch die Bestimmung über die bewaffnete Flugbegleitung („Sky marshals") geht sein Betätigungsfeld noch darüber hinaus.

Das Bundeskriminalamt (BKA) wird in dreifacher Weise gestärkt: Seine originäre Ermittlungszuständigkeit wird auf bestimmte Fälle der „Computersabotage" ausgedehnt. Lausch- und Spähangriffe des BKA dürfen seit Januar zum Schutz „eingesetzter Personen" stattfinden – bislang waren sie nur beim Einsatz „Verdeckter Ermittler" zulässig. Und in sogenannten „Initiativermittlungen" kann das Amt nun Daten direkt erheben, ohne die Landespolizeien beteiligen zu müssen.

Schlauer in fünf Jahren?

Einige der Novellierungen (Geheimdienstgesetze, G 10- und Sicherheitsüberprüfungsgesetz, ein Teil des BKA-Gesetzes) sind bis zum 10.1.2007 befristet. Damit sollte manchen ParlamentarierInnen und Landesregierungen wohl die Zustimmung erleichtert werden. Dass der internationale Terrorismus bis dahin verschwindet, glaubt niemand. Dass es eine redliche Evaluierung der neuen Kompetenzen geben wird, ist so unwahrscheinlich wie ein Lottogewinn. Und eine Regierung, die zugunsten von

Demokratie und Bürgerrechten die Sicherheitsapparate stutzt, die ist wohl auch in fünf Jahren nicht in Sicht.

Rasterfahndung

Gegenwärtige Gefahr für die Grundrechte

von Heiner Busch

Sich widersprechende Gerichtsurteile, eine von Land zu Land unterschiedliche Praxis, massenhaft Daten, aber keine Ergebnisse – das ist die Bilanz nach rund einem halben Jahr der Rasterfahndungen.

Ausländischen Studenten ist es zu verdanken, dass eine der gefährlichsten Ermittlungsmethoden der deutschen Polizei rechtlich hinterfragt wird: Aufgrund ihrer Klagen entschieden die Landgerichte Berlin und Wiesbaden am 15. Januar bzw. 6. Februar 2002, dass eine „gegenwärtige Gefahr" nicht bestehe und die Ende September letzten Jahres begonnenen Rasterfahndungen daher unzulässig seien.[1] Die beiden Gerichte stützten ihre Beschlüsse pikanterweise auf Erklärungen der Bundesregierung, „wonach keine Anzeichen dafür ersichtlich sind, dass die Verübung terroristischer Anschläge in der Bundesrepublik Deutschland bevorsteht". Dies habe sich auch nach der Entscheidung des Bundestages, deutsche Soldaten nach Afghanistan zu entsenden, nicht geändert. Sogenannte Schläfer – so heißt es in dem Wiesbadener Beschluss – seien in der BRD zwar entdeckt worden, „fortgeschrittene Planungen konkreter Anschläge konnten ihnen jedoch nicht nachgewiesen werden."

Dass die beiden Entscheidungen zu politischen Kontroversen führen würden, war absehbar. In Berlin erlebte die neue SPD-PDS-Koalition ihren ersten Streit in Sachen Innere Sicherheit: Innensenator Ehrhart Körting (SPD) beabsichtigte zunächst nur die Daten jener drei Studenten, die erfolgreich geklagt hatten, aus dem Abgleich herauszunehmen. An-

1 Landgericht (LG) Berlin, Beschluss v. 15.1.2002 – Az.: 84 T 278, 288, 289, 308, 309, 348-351/01, 84 T 8/02; LG Wiesbaden, Beschluss v. 6.2.2002 – Az.: 4T 707/01; beides auf www.cilip.de/terror

sonsten sei die Rasterfahndung bis zum endgültigen Entscheid des Kammergerichts weiter zu betreiben. Körting ist inzwischen zurück gekrebst, und die Daten lagern zur Zeit im Panzerschrank. Der Beschluss des höchsten Berliner Gerichts wird im April erwartet.[2]

In Hessen wurde die Rasterfahndung nach dem Beschluss des LG Wiesbaden zunächst ausgesetzt. Am 21. Februar verwarf das Oberlandesgericht (OLG) Frankfurt die Beschwerde von Innenminister Volker Bouffier (CDU). Daraufhin war die Operation gänzlich einzustellen, was dem Minister offensichtlich nicht gefiel. Hessen dürfe „nicht zum Rückzugsraum für potenzielle Terroristen und sogenannte Schläfer werden." Man werde prüfen, ob nicht kurzfristig die Bestimmungen des Polizeigesetzes zu ändern seien. Erst am 26. Februar bewilligte Bouffier die Löschung der „in monatelanger polizeilicher Arbeit" erhobenen Daten.[3]

Streit unter den Gerichten

Die hessische Polizeigesetz-Novelle ist trotzdem unterwegs.[4] Ihr Ziel ist die Absenkung der Eingriffsschwelle nach dem Vorbild des baden-württembergischen Polizeigesetzes, das die Rasterfahndung zur „vorbeugenden Bekämpfung von Straftaten mit erheblicher Bedeutung" zulässt. Bayern erlaubt sie „zur Abwehr" solcher Straftaten, Sachsen zu deren Verhinderung. Das Vorliegen einer (einfachen) konkreten Gefahr verlangen Niedersachsen, das die Rasterfahndung erst nach dem 11. September ins Gefahrenabwehrgesetz aufgenommen hat, und Bremen, das eine Woche vor den Attentaten in den USA die entsprechende Befugnis gestrichen hatte, um sie am 25. Oktober wieder einzuführen. Schleswig-Holstein erlaubt in seiner ebenfalls neuen Regelung die Rasterfahndung zur Abwehr einer erheblichen Gefahr.

Hessen gehört bisher zur Gruppe der restlichen zehn Bundesländer, deren Polizeigesetze eine „unmittelbar bevorstehende" (Hamburg) bzw. „gegenwärtige Gefahr für Leib, Leben, Freiheit einer Person oder für den Bestand oder die Sicherheit des Bundes oder eines Landes" als Eingriffs-

2 Süddeutsche Zeitung v. 25.1.2002

3 OLG Frankfurt, Beschluss v. 21.2.2002 – Az.: 20 W 55 02; Hessisches Ministerium des Innern: Presseerklärung v. 21.2.2002, Frankfurter Rundschau v. 24., 26. und 27.2.2002

4 Gesetzentwurf der Regierungsfraktionen CDU und FDP: „Änderung des HSOG zur Weiterführung der Rasterfahndung", LT-Drs. 15/3755

voraussetzung vorsehen.[5] Über die Frage, was dieser Begriff konkret bedeutet, streiten sich aber nicht nur die Sicherheitspolitiker, sondern auch die Gerichte. Für das OLG Frankfurt ist die „gegenwärtige Gefahr" die „höchste Steigerungsform des Gefahrenbegriffs"; „die Einwirkung des schädigenden Ereignisses" müsse „bereits begonnen haben oder die Einwirkung muss unmittelbar oder in allernächster Zeit mit an Sicherheit grenzender Wahrscheinlichkeit bevorstehen." Da in Deutschland keine Anschläge zu erwarten seien, sei die Rasterfahndung unzulässig.

Auch wenn solche Attentate nicht hierzulande, sondern irgendwo anders erwartbar seien, müsste – so das Verwaltungsgericht Mainz – die deutsche Polizei diese gegenwärtige Gefahr abwehren; eine absurde Vorstellung, denn leider ereignen sich permanent irgendwo auf der Welt schwerste Gewalttaten und Menschenrechtsverletzungen, gegen die die deutsche Polizei bisher nie etwas unternommen hat. Die „gegenwärtige Gefahr" mutiert damit zu einer Dauergefahr. Nicht umsonst erklärt das Gericht, „der Informationsabgleich erfolgt zur vorbeugenden Bekämpfung schwerster Verbrechen" und greift damit auf eine kaum begrenzbare Aufgabennorm zurück, die seit den 70er Jahren zusätzlich zur traditionellen Aufgabe der Gefahrenabwehr ins Polizeirecht Einzug hielt.[6]

Auch das OLG Düsseldorf sieht eine gegenwärtige Gefahr als gegeben. Die Polizei habe 42 Personen, die in Nordrhein-Westfalen leben oder gelebt haben, als „Unterstützer oder Kontaktpersonen im Netzwerk des Osama bin Laden" identifiziert. Die gegenwärtige Gefahr erfordere zwar ein „größeres Maß an zeitlicher Nähe" als die bloße konkrete Gefahr. „Ist allerdings der zu erwartende Schaden sehr groß, sind an die Wahrscheinlichkeit des Schadenseintritts nur geringe Anforderungen zu stellen." Es reiche aus, wenn „nur eine entfernte Möglichkeit des Schadenseintritts" bestehe. Allerdings hätten nur Ausländer und keine Deutschen gerastert werden dürfen.[7]

Unterschiedliche Kriterien

Seit den Gerichtsbeschlüssen in Berlin und Hessen ist die Rasterfahndung keine bundesweite mehr. Bundeseinheitlich war sie schon vorher

5 Gerling, R.W.; Langer, C.; Roßmann, R.: Rechtsgrundlagen zur Rasterfahndung, in: Datenschutz und Datensicherheit 2001, H. 25, S. 1-10

6 VG Mainz: Beschluss v. 19.2.2002 – Az.: 1L 1106101. MZ

7 OLG Düsseldorf Beschlüsse v. 8.2.2002 – Az.: 3Wx 351/01 und 357/01

nie gewesen, auch wenn sich anfangs die Landeskriminalämter – und der Verfassungsschutz – auf ein gemeinsames Täterprofil geeinigt hatten. Wie dieses Profil ausgesehen hat, lässt sich an der Anordnung des Berliner Amtsgerichts Tiergarten vom 20. September erkennen: „Männlich, islamische Religionszugehörigkeit ohne nach außen tretende fundamentalistische Grundhaltung, legaler Aufenthalt, keine eigenen Kinder, Studientätigkeit (technische Fächer), Mehrsprachigkeit, keine Auffälligkeiten im allgemeinkriminellen Bereich, rege Reisetätigkeit, häufige Visabeantragungen, finanziell unabhängig."[8]

Dieser Kriterienkatalog ist nicht nur diskriminierend, weil er definitiv unverdächtige Personen, nur weil sie zu einer bestimmten religiösen Gruppe gehören, unter Generalverdacht stellt. Er war auch nicht umsetzbar: „Erst nach Erlass des Beschlusses", so berichtet der Berliner Datenschutzbeauftragte, „stellte die Polizei fest, dass es bei Anlegung dieser Merkmale zu überhaupt keinen Trefferfällen kommen würde, weil keine der (zur Übermittlung) verpflichteten Stellen über alle diese Daten verfügt. Deshalb berichtigte der Amtsrichter am 21. September 2001 auf Antrag des Landeskriminalamtes den Beschluss dahingehend, dass die Merkmale der zu überprüfenden Personengruppe lediglich die Eigenschaften ‚vermutlich islamische Religionszugehörigkeit' und ‚vermutlich legaler Aufenthaltsstatus in Deutschland' ... umfassen."[9]

Gesucht wurde zunächst nach Personen aus vierzehn Staaten, die im Anhang des Beschlusses aufgeführt waren. Im weiteren Verlauf wurde die Liste auf insgesamt 28 Staaten ausgeweitet – darunter auch Bosnien, Frankreich und Israel. Anfangs sollten die Universitäten Daten von Personen übermitteln, die zwischen 1983 und 1996 immatrikuliert waren. Ende Oktober forderte die Polizei auch Angaben über Studenten aus der Zeit von 1960-1983 sowie aus dem aktuellen Wintersemester 2001/02.[10]

Erfassungsschwierigkeiten gab es auch in anderen Ländern. Die bayerischen Melderegister führen keine Hinweise auf islamische Religionszugehörigkeit. Eigens vermerkt werden nur katholisch, evangelisch und jüdisch, alle weiteren Konfessionen figurieren unter „andere".[11]

---

8 Amtsgericht Tiergarten: Beschluss v. 20.9.2001 – Az.: 353 AR 199/01

9 Der Berliner Beauftragte für Datenschutz und Informationsfreiheit: Jahresbericht 2001, Berlin 2002, Kapitel 4.1.1.

10 Berliner Zeitung v. 22.10.2001; AStA der Freien Universität: Info-Blatt v. 20.11.2001

11 Süddeutsche Zeitung v. 5.10.2001

In Brandenburg waren nur die wenigsten Melderegister überhaupt in der Lage, eine Auswahl vorzunehmen. Viele Gemeinden lieferten deshalb den gesamten Bestand ans LKA, dessen MitarbeiterInnen die Daten zum Teil gänzlich neu eingeben mussten. Auch hier erfolgte eine schnelle Ausweitung der Alterskriterien (ursprünglich 18-25, später 18-50-Jährige). Am 16. Oktober berichtete die „taz" von einer 30 Staaten umfassenden Liste, sechs Tage später war in der „Berliner Morgenpost" von 34 Staaten die Rede. Laut Datenschutzbericht wurden später nicht nur Staatenlose, sondern auch Deutsche mit Geburtsort im Ausland in die Rasterfahndung einbezogen, wodurch auch Eingebürgerte und Spätaussiedler erfasst wurden.[12] Hessen hatte 22 Staaten auf der Liste, Niedersachsen 23, Sachsen 35 (inkl. GUS-Staaten). Erfasst wurden hier auch Deutsche, die keiner der „öffentlich-rechtlichen Religionsgemeinschaften angehören" sowie Staatenlose und Flüchtlinge.[13]

In Nordrhein-Westfalen – so das Innenministerium – hatte die Polizei „vor Beginn der Rasterfahndung ... ermittelt, dass die Universitäten die Staatsangehörigkeit, das Geburtsland oder die Religionszugehörigkeit der Studenten nicht durchgängig in automatisierten Dateien erfassen."[14] Deshalb ließ man gleich die Daten aller zwischen 1960 und 1983 geborenen und zwischen 1983 und 1996 immatrikulierten übermitteln – ohne Rücksicht auf die Herkunft.

Abgesehen vom allgemeinen Feindbild haben die Rasterfahndungsaktionen in den einzelnen Bundesländern praktisch nur eine Gemeinsamkeit: Es handelt sich durchgängig um ein Massendatengeschäft. Das Baden-Württembergische LKA bezog von den Meldebehörden Daten über 270.000 Menschen, die Zahl der „Trefferfälle", also derjenigen Personen, die im Raster hängen blieben, ist nicht bekannt.[15] In Berlin wurden Daten über 58.000 Personen zusammengetragen, von denen 199 dem Profil entsprachen. Diese Zahl wurde – so Detlef Schmidt vom Datenschutzbeauftragten des Landes – weiter auf ca. 100 reduziert. Das Brandenburgische LKA erhielt von den diversen zur Übermittlung verpflichteten Stellen 460.270 Datensätze. Im November waren laut Daten-

12 Landesbeauftragter für Datenschutz und Informationsfreiheit: Tätigkeitsbericht 2001, Potsdam 2002, Kapitel 1.3.

13 Frankfurter Rundschau v. 11.1.2002; taz v. 16.10.2001; Sächsischer Ltg., Drs. 3/5294

14 Innenministerium NRW: Presse-Information v. 12.2.2002

15 Landesbeauftragter für den Datenschutz: Tätigkeitsbericht, Stuttgart 2002, S. 13

schutzbericht 19.000 Personen in der Datei „Rasterfahndung“ des LKA gespeichert. Am 25. März hieß es, die Aktion dauere noch an, 27.683 Menschen entsprächen den Kriterien.[16] Die Nordrhein-Westfälische Polizei, so das OLG Düsseldorf in den zitierten Beschlüssen, erhielt von den Einwohnermeldeämtern 4.669.224 Datensätze, vom Ausländerzentralregister 89.000 und von den 54 Universitäten und Fachhochschulen 474.515. Aus diesen destillierte sie rund 11.000 „Trefferfälle“.

In Hamburg wertete das LKA „die Daten von über 10.000 männlichen Studierenden“ aus. 140 von ihnen erhielten im Januar – nach Abschluss des elektronischen Abgleichs – eine Aufforderung zu einem „persönlichen Gespräch“ bei der Polizei. Es bestehe kein Zwang zu erscheinen; wer nicht komme, werde aber auf anderem Wege überprüft. Zu dem „Gespräch“ sollten die Betroffenen allerlei persönliche Unterlagen mitbringen: Ausweisdokumente, gegebenenfalls Heiratsurkunde und Geburtsurkunde der Kinder, Studienbescheinigungen der besuchten Universitäten, Fachhochschulen, Lehrgänge und Kurse, Arbeitsbescheinigungen, Praktikumsunterlagen, Unterlagen über Reisen, Kontoauszüge, Bescheinigungen über Vereinsmitgliedschaften ...[17]

Das BKA tritt auf den Plan

Das Bundeskriminalamt (BKA) hat eigens für die Rasterfahndung eine Datei „Schläfer“ eingerichtet, in der die Länder ihre „Trefferfälle“ speichern sollen. Im Februar umfasste die Datei 19.872 Personen, Nordrhein-Westfalen hält mit seinen 11.000 Datensätzen definitiv die Spitzenposition.[18] Einige Länder (z.B. Niedersachsen) hatten noch keine Fälle übermittelt, Berlin hatte seine nach dem Beschluss des Landgerichts bereits wieder gelöscht. Trotzdem dürften sich die Anteile der übrigen Bundesländer allenfalls im dreistelligen Bereich bewegen.

Die Datei soll u.a. dazu dienen, die „Grenzgängerfälle“ zusammenzuführen, also diejenigen Personen, die zwar die Kriterien der Rasterfahndung erfüllen, aber z.B. in einem Bundesland studieren, jedoch in einem anderen wohnen und daher nicht isoliert von einem Bundesland erkannt werden können. Für diese und ähnliche Auswertungen mit den

16 Berliner Morgenpost v. 25.3.2002
17 Der Tagesspiegel und taz v. 22.1.2002
18 BT-Drs. 14/8257 v. 18.2.2002

gelieferten Datensätzen konnte sich das BKA schon vor Inkrafttreten des neuen Anti-Terror-Gesetzes auf seine Zentralstellenkompetenz nach § 7 BKA-Gesetz stützen.

Es hat aber auch selbst – rechtswidrig – weitere Daten erhoben und mit denen der „Schläferdatei“ abgeglichen. Eigene Befugnisse für eine Rasterfahndung zu präventiven Zwecken fehlen im BKA-Gesetz. Der Generalbundesanwalt hatte eine auf die §§ 98 und 98a der Strafprozessordnung gestützte bundesweite Rasterfahndung, mit der er das BKA hätte beauftragen können, im letzten Jahr abgelehnt. Obwohl demnach auch keine richterliche Anordnung vorlag, hat das Amt dem Vernehmen nach an verschiedenste Stellen Briefe versandt, die den Eindruck erweckten, die Angefragten seien zur Herausgabe von Daten verpflichtet. Erst das im Januar in Kraft getretene Terrorismusbekämpfungsgesetz hätte es dem Amt erlaubt, von sich aus den von den Ländern zusammengetragenen Datenbestand durch eigene Erhebungen zu ergänzen.

Was nicht passt, wird passend gemacht

Das ist aber nicht der einzige Fall, wo Befugnisse vorzeitig ausgeübt wurden: In Brandenburg ordnete das Amtsgericht Eberswalde die Rasterung von Sozialdaten an – auch dies wäre erst nach dem Terrorismusbekämpfungsgesetz erlaubt gewesen. Niedersachsen begann die Rasterfahndung vor der Änderung des Gefahrenabwehrgesetzes – und zwar mit einer vertraulichen Anweisung des LKA. Das Berliner LKA fragte bereits am 17. September bei den Universitäten, beim Hahn-Meitner-Institut und bei den Wasserbetrieben an – drei Tage vor dem ersten, unbrauchbaren Beschluss des Amtsgerichts. Dass selbst die Freie Universität Berlin eilfertig dieser völlig unverbindlichen Anfrage nachkam, dass viele zur Übermittlung verpflichtete Stellen mehr Daten lieferten, als sie sollten, zeigt mit erschreckender Deutlichkeit, wie wenig das Recht und vor allem die Grundrechte in Zeiten des imaginierten Notstandes wert sind. Trotz des enormen Aufwandes hat die ganze Aktion nichts gebracht. Die Folgerung daraus kann nur lauten: Die Daten sind zu löschen und die Betroffenen zu informieren. Die Befugnisse zur Rasterfahndung dürfen nicht ausgebaut werden, sie sind ein für alle mal zu streichen.

Die arme Verfassung

Verfassungsschutz, V-Leute und NPD-Verbot

von Wolf-Dieter Narr

Seit Mitte Januar wird über sie geredet: Zuerst war's einer. Dann wurden es zwei, drei, schließlich fünf. Gemeint sind die V-Leute, die angeblich strikt im Sinne der freiheitlich demokratischen Grundordnung des Grundgesetzes die NPD ausspähten. Dazu waren und sind diese in der Wolle gefärbten NPD-Schafe trefflich geeignet.

In der Zwischenzeit weiß man eines ganz genau: dass nämlich niemand die Zahl der doppelten Lottchen, der gleichzeitigen V- und NPD-Leutchen ganz genau kennt. Und niemand scheint mehr genau zu wissen, worin nun der Skandal besteht. Darin, dass V-Leute als ‚gestandene' NPD-Leute „enttarnt" wurden; darin, dass dem Verfassungsgericht diese ‚beiläufige' Information nicht weitergeben wurde; darin, dass selbst der zuständige Innenminister keine Ahnung hatte; darin, dass V-Leute im amtlichen Verfassungsschutz eine solche Rolle spielen; darin, dass NPD und Verfassungsschutz V-Leute-kräftig zusammenarbeiten; darin, dass ein solcher in seinen V-Leuten und nationaldemokratischen Verflechtungen unübersichtlicher „Verfassungsschutz" die Verfassung als demokratisch grundrechtliche nicht schützen kann; oder darin – das ist die größte Sorge der BefürworterInnen und BetreiberInnen des NPD-Verbotsantrags –, dass das Verbot der NPD durch diese Affäre gefährdet werden könnte?

Fragen über Fragen. Sie hätten alle schon zuvor gestellt werden müssen und können, bevor der erste V-Mann dieser Serie – man muss sich den Ausdruck auf der Zunge zergehen lassen –, bevor also der Vertrauens-Mann Wolfgang Frenz in seiner Mehrfach-Identität erkannt worden ist und kollegialerweise noch weitere Enttarnungen nachzog. Bis dann niemand mehr wusste, woran er war, und das Verfassungsgericht das

Verbotsverfahren einstweilen aussetzte. Dabei hatte alles so schön mit vom Bundesverfassungsgericht trefflich ausgewählten Zeugen und Experten begonnen.

Apropos Bundesverfassungsgericht: Dieses spielt im Skandälchen, das um die V-Leute kreist – oder, wie man über zwei Monate nach der Skandalisierung in der Presse schon sagen muss, gekreist hat –, nur die Rolle einer missbrauchten Institution. Zu Unrecht. Dass das Gericht just die Kollegen Uwe Backes und Eckhard Jesse als Sachverständige für „Rechtsextremismus" oder, wie es nun abmildernd heißt, als „Sachkundige" bestellt hat, lässt seine eigene Kompetenz in reichlich trübem Licht erscheinen. Backes und Jesse, Herausgeber des Jahrbuches „Extremismus und Demokratie", gerieren sich nicht nur seit Jahren als wissenschaftliche Verfassungsschützer, sie sind auch stets treu den verfassungsschützerisch ausgegebenen Feindbildern gefolgt. Kein Wunder also, dass sie als gute Kalte Krieger noch 1990 der Meinung waren, der Extremismus von rechts werde „vielfach hoch-, der von links hingegen heruntergespielt."[1] Verlassen wir diesen Nebenschauplatz.

Im folgenden Überblick über das Skandälchen soll es um dreierlei gehen: um die nicht ermittelbare Zahl der V-Leute, die ‚amtlichen' Reaktionen und die nötigen weiteren, indes von (fast) niemandem gezogenen Konsequenzen.

Apropos V-Leute und NPD

Mit dem Verbotsverfahren gegen die NPD fängt alles an. Bundesregierung, Bundestag und Bundesrat haben mit überragender Mehrheit beim Bundesverfassungsgericht beantragt, die NPD gemäss Art. 21 Abs. 2 des Grundgesetzes zu verbieten. Um den Antrag zu begründen, griff man auf das Wissen jener Bundes- und Landesbehörden zurück, die man u.a. für solcherart potenziell nötige Verbote vor über 50 Jahren in der Alt-Bundesrepublik eingerichtet hat: die sogenannten und aufwendig gesammelten Erkenntnisse des Bundesamts und der Landesämter für Verfassungsschutz. Über die in der Verbotsbegründung enthaltenen „Erkenntnisse" hinaus wurden dem Verfassungsgericht vierzehn „Auskunftspersonen" genannt, die die Verfassungswidrigkeit in persona beweisen sollten. Soweit, so verbotsförderlich.

1 Frankfurter Rundschau v. 7.2.2002

Ende Januar 2002 drückte einen Beamten des Innenministeriums das zu einem ordentlichen Verfahren gehörige Gewissen. Er eröffnete dem Gericht, dass eine der vierzehn „Auskunftspersonen“ eine Doppelrolle spielen müsse, er sei NPD-Mitglied und zugleich V-Mann des Verfassungsschutzes. Die Rede war von Wolfgang Frenz. Das Bundesverfassungsgericht hat daraufhin den im Februar anstehenden Termin mündlicher Verhandlung abgesagt und das Verfahren einstweilen suspendiert.

Die Doppelrolle des Wolfgang Frenz, die dem Gericht zuvor nicht signalisiert worden war, brachte die hektische Suche nach weiteren in den Zeugenstand erhobenen Doppelkünstlern in Gang. Das eingangs genannte Zuwachsspiel begann. Otto Schily, Bundesminister des Innern, so hieß es am 5. Februar, „weiß von drei V-Leuten“.[2] Wenig später waren's deren fünf. Die Frankfurter Rundschau titelte am 16. Februar durchaus nicht ironisch: „Schily erbost über neue V-Leute. Späte Angaben der Länder für NPD-Verbot ärgern Minister.“ Von insgesamt 100 Leuten des Verfassungsschutzes, die die NPD auslugten, war bald die Rede. Einer, der die Zahlen kennen müsste, der frühere Präsident des Bundesamts für Verfassungsschutz und zeitweilige Innensenator des Landes Berlin, Ekkart Werthebach, sagte dazu: „Niemand kann diese Zahl im Moment präzise schätzen, weil dann alle Landesämter für Verfassungsschutz ihre Informationen über geführte V-Leute auf den Tisch legen müssten. Richtig ist aber, dass die NPD als jahrelang verfassungsfeindliche Partei sehr intensiv beobachtet worden ist von allen Verfassungsschutzbehörden. Deshalb ist die Zahl der V-Leute hoch.“[3]

Das Skandälchen wurde rasch handsam gestutzt, alle Problemsprossen wurden beschnitten. Zuerst bekam der Beamte, der seine Information an das Gericht nicht über ‚seinen' Minister geleitet hat, sein ‚Fett' weg; was mit ihm seither im Rahmen des Ministeriums geschehen ist, wissen wir nicht. Dann wurde der Fall Wolfgang Frenz in der Presse ausführlich vorgestellt. Wolfgang Frenz, seit 1995 nicht mehr für den Verfassungsschutz tätig, hatte seine Doppelrolle insgesamt 36 Jahre gespielt. Er hat es hierbei nicht nur zum hohen NPD-Funktionär gebracht; er hat sich vielmehr bis in jüngste Zeit rabiat national-„demokratisch“ – das heißt zugleich rabiat antisemitisch – geäußert und war „seit langem als

2 Frankfurter Rundschau v. 5.2.2002
3 Berliner Morgenpost v. 29.1.2002

Hardcore-Nazi bekannt."[4] Die drei Verfassungsgewalten Bundesregierung, Bundesrat und Bundestag, die die NPD anklagten, fanden diesen Umstand indes harmlos. In ihrer gemeinsamen Stellungnahme zum V-Mann-Problem, die sie Mitte Februar dem Gericht zuleiteten, unterstrich die bundesdeutsche Verfassungsgewalt-Triade, dass zwischen den V-Mann-Eigenschaften und den Aussagen oder Handlungen von V-Leuten in ihrer Eigenschaft als Rechtsextremisten und NPD-Mitgliedern strikt zu unterscheiden sei – analog einer perfekten Rollentrennung im Theater.[5] Schließlich wurde die „Panne" Frenz & Co. zu einem bloßen Verfahrensmangel und dem Gericht gegenüber verharmlost. Und verfassungswirklich besehen, scheint dies auch der Fall zu sein. So man denn angesichts der Abstimmung der Verfassungsschutzämter untereinander, des sogenannten Quellenschutzes etc. überhaupt dazu in der Lage wäre (s. oben das Werthebach-Zitat), hätte man dem Gericht rechtzeitig und erschöpfend signalisieren müssen, welche kunst- und also verbotsantragsgerechten Doppelrollenspieler es zu erwarten habe, damit es seinerseits entsprechend rollentrennerisch vorgehen und die Informationen exakt auseinander halten könne. An Künsten der Interpretation sollte es, so scheint es, keiner der drei Gewalten und ihrer diversen Ämter fehlen.

Das Verbotsverfahren

Das Verbotsverfahren stagniert. Es wird jedoch, so der Schein nicht trügt, nach den Wahlen „unpolitisch", sprich: im Konsens der ‚verfassungsgemäßen' Parteien, und dann ohne Irritationen durch den bis dahin längst vergessen gemachten Skandal in Karlsruhe seinen verfassungsgerichtlichen Gang nehmen.

In der oben zitierten „Gemeinsamen Stellungnahme" haben die Verbotskläger ihre Argumente wiederholt. Neue Aspekte sind nicht hinzugekommen. Auch außerhalb der klagenden Verfassungsorgane und ihrer Repräsentanten kam fast niemand darauf, ob an der Klage gegen die NPD etwas falsch sein könne, wenn man für ein Verbot der Partei V-Leute benutzen müsse – jene geradezu der „Natur der Sache" nach zweifelhaften Ehrenleute. Der Einsatz der Verbotswaffe ist im Grundgesetz mit

4 Frankfurter Rundschau v. 24.1.2002

5 Auszüge aus der gemeinsamen Stellungsnahme von Bundestag, Bundesrat und Bundesregierung zum V-Mann-Problem, in: Frankfurter Allgemeine Zeitung v. 16.2.2002

guten Gründen erschwert worden. Muss diese Waffe in der Tat erprobt werden, wenn man die Gefahr, die die NPD politisch öffentlich darstellt, durch spionageartige Techniken und V-Leute herausfinden muss – durch Techniken also, die selbst verfassungspolitisch, sprich demokratisch-grundrechtlich auf krummen Beinen gehen? Besteht der Missbrauch, den Bundesregierung, Bundestag und Bundesrat mit dem Verfassungsgericht durch ihre Verbotsklage betreiben, nicht primär darin, dass sie als exekutive und legislative Gewalten die judikative Gewalt unnötig einem – demokratisch-grundrechtlich gesehen – falschen Druck aussetzen?

Ausgelassen wurde in den Januar- und Februardiskussionen rund um die V-Leute und ihrer politische „Würde“ als Zeugen auch die Frage nach der Institution der Verfassungsschutzämter selber und deren Funktionen. Diese Frage hätte vor aller grundsätzlichen Kritik schon bei zwei im Januar/Februar sichtbar werdenden Auffälligkeiten anzuheben: Wie können die Verfassungsschutzämter die Verfassung schützen, wenn schon die zuständigen Organe, in deren Rahmen sie tätig sind, die Innenministerien und ihre Spitzenrepräsentanten nämlich, nicht genau wissen, woran sie sind und was sie tun, wenn sie daran gehen, mit dem Verfassungsschutz die Verfassung zu schützen? Die Kontroverse um den Schwarzen Peter „V- und NPD-Mann in einem“ zwischen den Innenministern Schily, Beckstein und Schäuble ist dafür symptomatisch.

Das Kontrollproblem geht weiter: Auch die Ämter selber haben ihre Schwierigkeiten: Um ihre „Quelle“, V-Mann X (selten V-Frau Y) zu schützen, muss auch im jeweiligen Amt und vor allem zwischen den Ämtern ein großes Maß an „Vertrauensschutz“ den „Vertrauens“-Leuten gegenüber geübt werden. Es scheint, als müsse letztlich die Vertrauensperson in sich selbst, in ihrer dritten Identität, ausmachen, ob ihr Doppelrollenspiel so ausgeübt wird, dass die Rolle als verfassungsschützende Vertrauensperson diejenige der an potentiell verfassungsfeindlichen Aktivitäten mitwirkenden Person überwiegt oder dass doch beide „strikt“ von einander zu trennen sind.

Die parlamentarischen Kontrollkommissionen haben ohnehin immer das Nachsehen. Es bleibt ihnen nichts anderes übrig, als hinterher nachzuschauen, was jeweils aus der verfassungsschützerisch und vertrauensleutehaft gefüllten Pandora-Büchse herausfällt.

Schützen geheimdienstliche Ämter die Verfassung?

Das ist die Frage. Sie wurde in all dem V-Leute-Gewusel der letzten Monate nicht einmal gestellt (Ausnahmen bestätigen wie üblich die Regel). Selbst kompetente und kritische Beobachter wie der Verfassungsrechtler Erhard Denninger dringen zu ihnen nicht (mehr) vor. Als verstehe sich – nimmt man das Grundgesetz ernst – von selbst, dass es eines administrativen Verfassungsschutzes bedürfe. Und als verstünde es sich konsequenterweise außerdem von selbst, dass dieser Geheimdienst das nicht mehr kontrollierbare Instrument der V-Leute benötige.

Welch ein widersprüchlicher Ausdruck, ein orwellscher Euphemismus: Vertrauensleute. Letzteren ist, wie die im Januar dieses Jahres erzählte Fabel lehrt, aus einem doppelten Grunde nicht zu trauen. Damit sie in „Untergründe" gelangen, zu denen selbst eine „normale" geheimdienstlich tätige Person keinen Zugang hat, müssen sie möglichst aktive Mitglieder solcher Gruppen werden, die man „im Dunkeln" nicht sieht. Selbst wenn diese Leute, erst um ausspionieren zu können, etwa NPD-Mitglieder werden und dort ihre Sporen durch besonderes stiefelgesporntes Verhalten erringen, steht die Chance, über kurz und vor allem über länger korrupt zu werden, sagen wir 10 zu 1. Das kennt man aus vielen Bereichen polizeilicher und geheimdienstlicher Tätigkeit. Der andere Grund, dass die Vertrauensleute gerade solche sind, denen man jedenfalls grundrechtlich nicht vertrauen kann, besteht darin, dass niemand sie in ihrem Verhalten und in dem, worüber sie informieren, zureichend kontrollieren kann (auch nicht, wenn man mehrere V-Leute in vollem Vertrauen gegeneinander hetzt).

Nun mag es Bereiche geben, wo man das Risiko der Spionage und der Gegenspionage eingehen muss. Das ist hier nicht mein Thema, obgleich meine empirisch vielfach bestätigten und demokratisch-politisch systematisch entwickelten Zweifel groß sind. Wozu braucht jedoch der Verfassungsschutz solche, wie es in einem anderem euphemistischen Deckwort heißt, „nachrichtendienstliche Mittel"?

Bevor ich die Antwort auf diese Frage nachfolgenden andeute, will ich nur auf den täuscherischen Fehlversuch hinweisen, V-Leute dadurch verfassungsgemäß salonfähig zu machen, dass man sie ‚besser' verrechtlicht. In diese Kerbe schlagen nicht wenige neuere Einlassungen von Roderich Reifenrath bis Arthur Kreutzer.[6] Wie solche erfahrenen Leute

6 Frankfurter Rundschau v. 6.2.2002 und 16.3.2002

zu solchen verfehlten Reformvorstellungen einer zusätzlichen Verrechtlichung kommen, bleibt ein Rätsel. Man sollte ja nicht annehmen, sie jagten der Gesetzesillusion nach. Reifenrath und Kreutzer wissen sehr wohl, dass die meisten Bundesdeutschen kritisch verstummen, wenn behauptet wird, etwas sei „rechtsstaatlich". Ebenso wenig mag man Naivität unterstellen. Wie kann jemand vernünftigerweise annehmen, der V-Leute-Einsatz, der der „Natur der Sache" und der Personen nach gerade nicht genau und offen erfasst werden soll und kann, sei rechtlich zu vertäuen. Es sei denn, man verfahre wie bereits in einigen Landesverfassungsschutzgesetzen und arbeite vor allem mit unbestimmten Rechtsbegriffen. Das aber bedeutet: Indem man den Anschein des gesetzlich Berechenbaren gibt, nimmt man gesetzesfaktisch alles bürgerlich Berechenbare, Rechtssichere und gerichtlich Überprüfbare hinweg. Das ist neuerdings die Eigenschaft allzu vieler Gesetze in Sachen „innere Sicherheit". Sie legalisieren das exekutivische Opportunitätsprinzip.

Es ist schlicht unmöglich, den Nachweis zu erbringen, dass man in einer liberalen Demokratie, die diese Kennzeichnung verdient, eines administrativen Verfassungsschutzes bedürfe, der vor allem die eigenen Bürgerinnen und Bürger mit besagten „nachrichtendienstlichen Mitteln" ausspäht, aushorcht, erfasst und Erfasstes als „Erkenntnisse" im Rahmen der Exekutive weitergibt. Die bundesdeutsche Legitimationsformel mit falschem Verweis auf die Weimarer Republik, dass eine Demokratie „streitbar" bzw. „abwehrbereit" dem jakobinischen Motto „Keine Freiheit den Feinden der Freiheit" folgen müsse, führt in die Irre. Sie schädigt den Grundrechtsschutz und damit den Kern der Demokratie. Läse man die Botschaft der missbrauchten V-Leute im Rahmen des NPD-Verbotsverfahrens verfassungsgemäß, es könnte nur eine Konsequenz gezogen werden: Der administrative Verfassungsschutz gefährdet die lebendige Verfassung selber. Er ist ersatzlos abzuschaffen.

Wolf-Dieter Narr lehrt Politikwissenschaft an der Freien Universität Berlin und ist Mitherausgeber von Bürgerrechte & Polizei/CILIP.

Inland aktuell

Rot-rote Koalitionsvereinbarung in Berlin

SPD und PDS haben sich im Dezember 2001 auf eine Koalitionsvereinbarung für die Hauptstadt geeinigt. Über weite Strecken folgen die Koalitionäre dem Mainstream bundesrepublikanischer innerer Sicherheitspolitik, etwa in der Betonung von Prävention, der gewünschten intensiveren Zusammenarbeit mit dem Bundesgrenzschutz oder mit privaten Sicherheitsdiensten, den angestrebten Auslagerungen und Teilprivatisierungen, der Straffung der Polizeiorganisation etc. Die Feststellung, dass Sicherheit „neben dem Schutz vor Kriminalität ... auch den Schutz des Einzelnen und der Öffentlichkeit vor unverhältnismäßigen staatlichen Eingriffen“ umfasse, gehört in den Bereich allgemeiner politisch-rhetorischer Bekenntnisse. In einigen Fragen verspricht die neue Regierung jedoch, einen Weg in die richtige Richtung einschlagen zu wollen. Zu diesen erfreulichen Elementen des Koalitionsvertrages gehören:

- Die weitere Verschärfung des Demonstrationsrechts wird abgelehnt.
- In Berlin wird es keine Videoüberwachung öffentlicher Straßen und Plätzen geben.
- Die Reiterstaffel wird aufgelöst. (Mittlerweile hat Pferdefreund Schily die Tiere samt ihrer Reiter in den Bundesgrenzschutz übernommen.)
- Zukünftig sollen „Berliner Polizeibeamte eine individualisierbare Kennung gut sichtbar an ihrer Uniform tragen“. (Die Gewerkschaft der Polizei hat bereits ihren Widerstand angekündigt.)
- Durch die Novellierung des Berliner Polizeirechts (ASOG = Allgemeines Sicherheits- und Ordnungsgesetz) sollen die verdeckten Polizeimethoden „an einen Straftatenkatalog gebunden und nicht mehr auf eine Generalklausel gestützt“ werden. Außerdem verpflichtet sich der Senat, dem Parlament „jährlich einen detaillierten Bericht über Umfang und Erfolg“, insbesondere über verdachtsunabhängige Kontrollen und die akustische Überwachung, vorzulegen.
- Der Verfassungsschutz soll „zu einem Instrument moderner, wissenschaftlicher Beratung für Politik und Öffentlichkeit“ „fortentwickelt“ werden – wobei vollkommen offen bleibt, wie dies geschehen soll.

Die neue Koalition hat damit einige Absichten festgeschrieben, die an die (ehemals) grüne Programmatik erinnern; originellerweise ohne die Grünen. Es bleibt abzuwarten, was die Berliner Politik daraus macht.
(Norbert Pütter)

Anklage gegen BGS-Beamte nach tödlicher Abschiebung

Am 28.5.1999 starb Aamir Ageeb während seiner Abschiebung auf dem Lufthansaflug von Frankfurt a.M. nach Kairo. BGS-Beamte hatten den 30-jährigen Sudanesen gefesselt, ihm einen Helm aufgesetzt, und ihn solange in den Sitz gedrückt, bis er erstickte. Die drei Bundesgrenzschützer wurden nun wegen fahrlässiger Tötung von der Frankfurter Staatsanwaltschaft angeklagt. In mehreren medizinischen Gutachten wird ein „lagebedingter Erstickungstod" als Todesursache benannt. In ähnlichen Fällen waren bislang rechtsmedizinische Gutachten erstellt worden, die „lagebedingte Erstickungen" – als Resultat erstickungsgefährlicher Vorgehensweisen durch Polizeibeamte – ausblendeten: Nach dem Tod des Nigerianers Kola Bankole 1994, der nach einer „Beruhigungsspritze" und nach Knebelung auf dem Frankfurter Flughafen verstarb, wurden die Verfahren gegen die verantwortlichen Beamten eingestellt; der Arzt wurde freigesprochen, weil das gerichtsmedizinische Gutachten einen „plötzlichen Tod aus natürlicher innerer Ursache" bescheinigte. Nach dem Tod des Nigerianers Agbai-John 1995 in Frankfurt wurden „Rauschmittel" als Todesursache angegeben. Ein späteres Gutachten bescheinigte einen Erstickungstod. Im Fall Ageeb veranlasste die Staatsanwaltschaft eine genaue Rekonstruktion der Ereignisse im Flugzeug; ZeugInnen wurden befragt. Eine Verurteilung der Angeklagten wäre ein Präzedenzfall. Der Prozessbeginn ist noch offen. – In Wien wurden am 15.4.2002 drei Polizisten wegen fahrlässiger Tötung zu einer achtmonatigen Bewährungsstrafe verurteilt. Der Nigerianer Marcus Omoufuma war am 1.5.1999 während seiner Abschiebung erstickt.

Auf der Grundlage eines Berichtes der Schweizerin Gaby Vermot hat die Parlamentarische Versammlung des Europarats im Januar dieses Jahres die 43 Mitgliedstaaten zu einer sofortigen Einstellung menschenrechtsverletzender Abschiebepraktiken aufgefordert. Europaweit starben von 1991 bis 2001 13 Personen bei ihrer Abschiebung, davon allein 10 in den letzten zwei Jahren. Der Bericht kritisiert insbesondere den juristischen Graubereich, in dem Zwangsabschiebungen europaweit durchge-

führt werden. Zugleich werden länderspezifische Fallbeispiele tödlicher Abschiebungen dargestellt.[1]

Todesfall nach Pfeffersprayeinsatz in Hamburg

In der Nacht zum 8. März 2002 verstarb in Hamburg ein Mann nach einem Polizeieinsatz. Die wegen einer Schlägerei in einer Wohnung alarmierten Polizeibeamten hatten Reizgas und Pfefferspray eingesetzt, um einen Widerstand leistenden Mann zu überwältigen. Dieser ging zu Boden, worauf ihm die Beamten Handfesseln anlegten und ihn auf den Bauch drehten. „Plötzlich begann er zu verkrampfen und kollabierte", heißt es in der Erklärung der Polizeipressestelle. Der 39-Jährige, der sich kurz zuvor Kokain injiziert haben soll, verstarb trotz Reanimationsmaßnahmen durch einen Notarzt. Auch nach einer Eilsektion durch das Institut für Rechtsmedizin blieb die Todesursache noch unklar; der Fall wurde als Todesermittlungsverfahren an die Staatsanwaltschaft Hamburg abgegeben.

Pfefferspray kann starkes Brennen der Augen, Blindheit bis zu 30 Minuten, Haut- und Schleimhautbrennen, Atemnot, Krämpfe im Oberkörper, Würgereiz oder akute Kreislaufstörungen verursachen. Im Zusammenhang mit Vorerkrankungen (z.B. Asthma) sowie mit Drogenkonsum kann Pfefferspray tödlich wirken. Wegen eventueller Synergieeffekte wird davor gewarnt, das Spray zusammen mit anderen Reizstoffen zu verwenden. In den USA wurden 61 Todesfälle zwischen 1990 und 1995 mit dem Einsatz von Pfefferspray in Zusammenhang gebracht.[2]

Mittlerweile sind alle Bundesländer einer Empfehlung der Innenministerkonferenz von 1999 gefolgt und haben ihre Polizeien mit Pfefferspray ausgerüstet. Der Hamburger Fall verdeutlicht, dass das Spray keineswegs so ungefährlich ist, wie seit der Einführung behauptet wird. Die Anwendung in einem geschlossenen Raum, die Koppelung von Reizgas und Pfefferspray sowie die Einwirkung gegenüber einem Drogenkonsumenten sind genau die durch ExpertInnen angemahnten tödlichen Risiken, die im Hamburger Fall zusammengefallen sind.
(beide: Marion Knorr)

---

1 Der Bericht ist abrufbar unter: http://stars.coe.fr/ta/ta02/edir579.htm.

2 vgl. Wright, S.: Pfefferspray „gefährdet die Gesundheit", in: Bürgerrechte & Polizei/CILIP 69 (2/2001), S. 70-79

Fernmelde- und Postkontrolle nach dem G 10-Gesetz

Im Februar dieses Jahres legte das Parlamentarische Kontrollgremium (PKG) des Bundestages seinen jährlichen Bericht über die Post- und Fernmeldekontrolle durch das Bundesamt für Verfassungsschutz (BfV), den Bundesnachrichtendienst (BND) und den Militärischen Abschirmdienst (MAD) vor (BT-Drs. 14/8312). Durch die Neufassung des G 10-Gesetzes, die am 29.6.2001 in Kraft trat, ist das PKG nicht mehr nur verpflichtet, über die Anordnungen im Bereich der strategischen Fernmeldeüberwachung durch den BND zu berichten, sondern auch über Art und Umfang der individuellen Post- und Fernmeldekontrollen durch die drei Geheimdienste. Im Berichtszeitraum 1.7.2000 bis 30.6.2001 hat sich nur das BfV Überwachungsmaßnahmen genehmigen lassen. BND und MAD haben weder neue Kontrollen beantragt noch frühere verlängert. Der Bericht nennt 39 bis 46 Anordnungsverfahren, in denen 230 bis 247 Personen von Postkontrolle und Telekommunikationsüberwachung betroffen waren. Die Zahl schwankt, da die Anordnungen nicht jeweils für den gesamten Berichtszeitraum bestanden, sondern befristet waren. Anlass waren im Wesentlichen der Verdacht auf Straftaten im Bereich „Gefährdung des demokratischen Rechtsstaats“ und „Straftaten des Landesverrats und der Gefährdung der äußeren Sicherheit“. 27 Verfahren wurden im Berichtszeitraum beendet, jedoch wurde lediglich 10 Personen mitgeteilt, dass sie überwacht wurden. Da im Durchschnitt fünf bis sechs Personen pro Verfahren betroffen waren, betraf dies vermutlich nur wenige Verfahren.

Im Bereich der strategischen Fernmeldeüberwachung der internationalen nicht leitungsgebundenen Telekommunikation hat der BND weiterhin auf den Gebieten „Proliferation von ABC-Waffen“ sowie „Internationaler Rüstungshandel und -produktion“ die Satelliten- und Richtfunkkommunikation mittels bestimmter Suchworte überwacht. Dabei hat es 555 „nachrichtendienstlich relevante“ Meldungen im Bereich Proliferation gegeben und nur noch 24 aus dem Rüstungshandel, weshalb diese Überwachung im Januar 2001 eingestellt wurde. Die meisten Treffer stammen dabei aus dem Telefaxverkehr, Telexe seien mittlerweile zu vernachlässigen. Bei der Sprach-Telefonie hat man seit jeher wegen technischer Probleme kaum „Erfolge“ gehabt.
(Martina Kant)

Meldungen aus Europa

Terrorismus-Definition und die Folgen

Die am 6. Februar auch vom Europäischen Parlament gebilligte Terrorismus-Definition der EU zwingt die Mitgliedstaaten zur Einführung eines Tatbestandes der „terroristischen Vereinigung“ und erlaubt es, typische Handlungsformen militanten Protests (u.a. Haus- und Platzbesetzungen) als „terroristisch“ zu kriminalisieren.[1] Bürgerrechtliche Kritik an diesem Rahmenbeschluss hatte der Rat durch hastig eingebaute Bekundungen abzufedern versucht: „Grundrechte wie die Versammlungs-, Vereinigungs- oder Meinungsfreiheit“ würden nicht geschmälert.

Zwei Initiativen der spanischen Präsidentschaft, die erstmals am 29. Januar eingereicht wurden, zeigen, wie wenig solche Beschwichtigungsformeln taugen. Beide Initiativen wurden in der Terrorismus-Arbeitsgruppe des Rates präsentiert, in der die politischen Polizeien und Geheimdienste oder – wie es im Text heißt – „Vertreter und Experten der den Justiz- bzw. Innenministerien unterstellten Dienststellen vereint sind, deren Aufgabe die Bekämpfung des Terrorismus ist.“ Um eine bessere Koordination der mysteriösen Dienststellen zu erreichen, will die spanische Regierung zum einen ein Standardformular für den Nachrichtenaustausch über das BDL-Netzwerk, das chiffrierte Kommunikationssystem der Inlandsgeheimdienste, einführen.[2] Kommuniziert werden soll über „Vorfälle im Zusammenhang mit radikalen gewalttätigen Gruppen, die Verbindungen zum Terrorismus aufweisen.“ Die Terrorismus-Arbeitsgruppe habe „im Laufe ihrer Arbeit feststellen müssen, dass es während verschiedener Veranstaltungen und Gipfeltreffen der Europäischen Union zu einem stetigen Anstieg von gewaltsamen Ausschreitungen und Vandalismus durch radikale Gruppen gekommen ist, die in der Gesellschaft eindeutig ein Gefühl des Schreckens hervorgerufen haben.“ Eine entsprechende „Tatbestandsdarstellung“ habe die EU in der Terro-

1 Bürgerrechte & Polizei/CILIP 70 (3/2001), S. 56-58; Ratsdok. 14845/1/01
2 Ratsdok. 5712/02 (2. Revision v. 13.3.2002)

rismus-Definition geliefert. „Die Taten werden aus einem diffusen Umfeld heraus von Personen begangen, die unter dem Deckmantel unterschiedlicher gesellschaftlicher Gruppen auftreten." Dieses Umfeld missbrauche seinen legalen Status und helfe „Terrororganisationen, die als solche bereits in der EU bekannt sind", bei der Durchsetzung ihrer „ureigensten Ziele".

Der Datenaustausch sei ein „nützliches Instrument für die Verhütung und gegebenenfalls Verfolgung gewaltgeprägter, im städtischen Umfeld verübter Aktionen radikaler Jugendlicher". Im Prinzip soll er sich auf Personen beziehen, die „im Zusammenhang mit terroristischen Straftaten" vorbestraft sind. Allerdings könne „jedes Land im Einklang mit seinen nationalen Rechtsvorschriften Informationen über Personen austauschen, die zwar die genannten Voraussetzungen nicht erfüllen, deren Verbindung mit den erwähnten Terrororganisationen aber bekannt ist." Auch Europol könne gegebenenfalls weitere Daten beitragen.

Mit ihrer zweiten Initiative will die spanische Regierung vom Rat eine Empfehlung für den Ad-hoc-Einsatz von „multinationalen Ermittlungsgruppen".[3] Gemeint sind damit keineswegs gemeinsame Ermittlungsgruppen nach Art. 13 des (bisher nur von Portugal ratifizierten) EU-Rechtshilfe-Übereinkommens, die bei aller „Flexibilität" immer noch einen Bezug zum Strafverfahren aufweisen. Der spanischen Präsidentschaft geht es vielmehr um „operative außer- oder vorgerichtliche Ermittlungen", an denen sie nicht nur die Polizei, sondern auch „Sicherheitsdienste" beteiligen will. Entsprechende Teams sollen gezielt „für Ermittlungen, die Beschaffung und den Austausch von Informationen, Fahndungen, Lokalisierungen und generell bei sonstigen konkreten Operationen" gebildet werden. Wenn es gewünscht werde, sollten Europol-Mitarbeiter das Team analytisch und logistisch unterstützen.

EU-weite Rasterfahndung

Um einen Export heimischer Methoden auf die Ebene der EU bemüht sich auch die BRD.[4] Bereits im Oktober forderte sie den Aufbau eines EU-weiten und jeweils nationaler Ausländerzentralregister. Über eine solche Datenbank verfügt außer Deutschland bisher nur ein EU-Staat (Luxem-

3 Ratsdok. 5715/02 (2. Revision v. 11.3.2002)
4 Ratsdok. 13176/01 und 6403/02

burg). Weitere Vorschläge wurden in Deutschland in dem am 1. Januar in Kraft getretenen „Terrorismusbekämpfungsgesetz“ verankert: Verwendung von Eurodac-Daten (Fingerabdrücke von Flüchtlingen) für polizeiliche Zwecke, Visa-Entscheidungs-Dateien mit polizeilichem und geheimdienstlichem Zugriff, neue Methoden der „Identitätssicherung“.

Die Forderung, EU-weit Rasterfahndungen zu ermöglichen, wurde im neuen Jahr weiter konkretisiert. In einem „Vermerk“ vom 8. März lobt die deutsche Delegation die Rasterfahndung als „geeignetes und erforderliches Mittel im Kampf gegen den internationalen Terrorismus“ und stellt die hiesigen rechtlichen Bedingungen (im Polizeirecht und in der Strafprozessordnung) dar. Deutschland fordert von den anderen EU-Staaten mitzuteilen, ob sie ähnliche Verfahren praktizieren, ob sie „Hindernisse“ für die Einführung der Rasterfahndung sehen und „welche Voraussetzungen ... beachtet werden müssen, um ein europaweit einheitliches Vorgehen zu ermöglichen.“ Über die fehlenden Ergebnisse der deutschen Rasterfahndungen sowie über die ablehnenden Gerichtsentscheidungen aus Hessen und Berlin schweigt sich der Vermerk aus.

Planungen für das SIS II

Mit dem Wind des 11. Septembers im Rücken hat die SIS-Arbeitsgruppe des Rates die Planungen für das Schengener Informationssystem der zweiten Generation erheblich vorangetrieben. Das System wird technisch von der EU-Kommission entwickelt und über den Gemeinschaftshaushalt finanziert. Der Rat nahm hierzu am 6. Dezember eine Verordnung (1. Säule) und einen Beschluss (3. Säule) an.[5]

Auch hinsichtlich der „Anforderungen“ an das SIS II[6] sind wesentliche Entscheidungen bereits gefallen oder zumindest vorgezeichnet. Dies betrifft zum einen die Frage, welche zusätzlichen Stellen Zugang zum SIS II erhalten sollen. Weitgehend einig ist man sich über Zugriffsrechte für Eurojust und Europol. Hier bedürfte es zusätzlicher technischer Vorkehrungen, da diese beiden Institutionen nicht über eine nationale SIS-Komponente angeschlossen werden können. Für den technischen Aufbau des SIS irrelevant sind dagegen Zugriffsmöglichkeiten weiterer nationaler Stellen: Grundsätzlich abgesegnet ist der Anschluss von Kraftfahrzeugre-

5 Amtsblatt der Europäischen Gemeinschaften, Nr. L 328 v. 13.12.2001, S. 1-6
6 Ratsdok. 6164/5/01, 13269/01, 14094/01, 14790/01, 5968/02, 5969/02, 5970/02

gisterbehörden, „Behörden, die Aufenthaltstitel erteilen“, sowie Staatsanwaltschaften bzw. Untersuchungsbehörden. Debattiert wird noch, ob Asylbehörden nach Aufbau von Eurodac den Zugang zum SIS brauchen, ob Sozialämter auf Daten über gestohlene, ungültige bzw. gefälschte Identitätspapiere zum Zweck der „Bekämpfung grenzüberschreitender Finanzkriminalität“ (d.h. unrechtmäßigem Sozialhilfebezug) haben sollen und ob nicht-staatliche Stellen, konkret: zentrale Auskunftstellen des Kreditwesens (SchuFa) am SIS beteiligt werden dürfen. Der Zugang von Inlandsgeheimdiensten zum Zweck der „Terrorismusbekämpfung“ wird noch geprüft. Grundsätzlich steht der Rat diesem Vorhaben positiv gegenüber.

Weit fortgeschritten ist auch die Debatte über neue Datenkategorien und „Funktionalitäten“: So sollen Ausschreibungen von Personen, Fahrzeugen und sonstigen Sachen miteinander verknüpft und Abfragen anhand unvollständiger Daten ermöglicht werden. Neue Kategorien wird es zum einen für die Sachfahndung geben (Schiffe, Flugzeuge, Container, ungültige, ge- und verfälschte Identitätsdokumente, Fahrzeugscheine, Visa, Schecks und Aktien, ggf. Kunstgegenstände und Tiere).

Fahnden will man ferner nach Personen, denen die Ausreise verboten ist (minderjährige Kinder, Strafgefangene auf Hafturlaub). Gegen eine Kategorie „potenziell gewalttätige Randalierer“ (Verhinderung der Teilnahme an Demonstrationen oder Fußballspielen) haben Schweden, Finnland und Norwegen noch Vorbehalte. Geprüft wird ferner, ob Nicht-EU-BürgerInnen bei der Einreise automatisch im SIS zu speichern sind oder ob diese Daten nicht besser in einer eigenständigen, aber mit dem SIS verlinkten Datenbank zu erfassen wären. Grundsätzlich einig ist sich der Rat, dass Daten über Visaerteilungen ausgetauscht werden sollen; unklar ist, ob dieser Austausch über das SIS erfolgen soll. Noch offen ist ferner, welche erkennungsdienstlichen Daten im SIS selbst gespeichert werden (ggf. Fotos) und ob zusätzliche Links zu nationalen Datensystemen (Fingerabdrücke, biometrische Daten, DNA-Profile) gesetzt werden dürfen. Als Reaktion auf den 11. September ist auch eine zusätzliche Datenbank über „Terroristen“ im Gespräch, die im Rahmen des SIS errichtet werden soll, auf die aber nur Geheimdienste und politische Polizeien zugriffsberechtigt wären. Das ursprüngliche SIS entsprach dem Konzept eines polizeilichen Fahndungssystems. Das SIS II droht zu einer Allround-Datenbank für den „Sicherheitsbereich“ zu werden.
(Heiner Busch)

Chronologie

zusammengestellt von Andrea Böhm

November 2001

02.11.: **Freispruch für Sachsens Datenschützer**: Das Landgericht (LG) Dresden spricht den sächsischen Datenschutzbeauftragten Thomas Giesen vom Vorwurf des Geheimnisverrats frei. Giesen wurde vorgeworfen, im August 2000 auf einer Pressekonferenz unberechtigt aus Aktenvermerken des damaligen Justizministers Steffen Heitmann (CDU) zitiert zu haben. Die Notizen dokumentierten, dass Heitmann 1997 einem CDU-Parteifreund Auskunft über ein Ermittlungsverfahren erteilt hatte.

09.11.: **Erste Anti-Terror-Gesetze verabschiedet**: Zwei Monate nach den Anschlägen in den USA stimmt der Bundestag der Streichung des Religionsprivilegs aus dem Vereinsrecht und dem sogenannten 3-Milliarden-Programm für mehr Sicherheit zu.
Gewaltschutzgesetz gebilligt: Der Bundestag beschließt ein Gesetz, das Frauen und Kinder besser vor gewalttätigen Familienvätern schützen soll. Damit können Opfer häuslicher Gewalt künftig in der eigenen Wohnung bleiben, während der Schläger ausziehen muss.

13.11.: **Urteile im La-Belle-Prozess gesprochen**: Wegen des Anschlags auf die Diskothek „La Belle“ im Jahre 1986 verurteilt das LG Berlin vier Angeklagte wegen Mordes, Mordversuchs und Beihilfe zum Mord zu Freiheitsstrafen zwischen 12 und 14 Jahren. Eine fünfte Angeklagte wird freigesprochen. In der Urteilsbegründung wird dem Staat Libyen eine erhebliche Mitverantwortung für die Tat bescheinigt.
Revision gegen Verurteilung von BGS-Beamten verworfen: Das Oberlandesgericht (OLG) Zweibrücken bestätigt ein Urteil des LG Landau gegen vier Beamte des Bundesgrenzschutzes (BGS), die einen togolesischen Asylsuchenden bei einer Kontrolle misshandelt hatten. Die Beamten waren zu Bewährungsstrafen zwischen 6 und 15 Monaten verurteilt worden.

14.11.: **Sicherheitskooperation vereinbart**: Bundesinnenminister Otto Schily und Thüringens Innenminister Christian Köckert unterzeichnen eine Vereinbarung, die eine engere Zusammenarbeit des Bundesgrenzschutzes (BGS) und der thüringischen Landespolizei bei der Kriminalitätsverhütung und -bekämpfung vorsieht.

15.11.: **Strafe für Drogenhändler vermindert**: Das LG Augsburg verkürzt eine ursprünglich vierjährige Freiheitsstrafe für einen Drogenhändler um die Hälfte und setzt die Reststrafe zur Bewährung aus. Der von der Polizei des Handels mit Haschisch verdächtige Mann war von einem polizeilichen Lockspitzel zu einem Heroingeschäft verleitet worden. Das Gericht beruft sich dabei auf eine Grundsatzentscheidung des Bundesgerichtshofs (BGH).
Entscheidung im Fall „Mehmet" verkündet: Der bayerische Verwaltungsgerichtshof erlaubt die Rückkehr des vor drei Jahren in die Türkei abgeschobenen Serienstraftäters Muhlis A. nach Deutschland. Das Gericht begründet sein Urteil mit dem europäisch-türkischen Assoziationsvertrag und der positiven Prognose eines Gutachters. Der unter dem Namen „Mehmet" bekannt gewordene Minderjährige hatte bis zu seinem 14. Geburtstag 62 Straftaten begangen.

20.11.: **Prozessbeginn gegen Beteiligte der Rostocker Krawalle**: Neun Jahre nach den ausländerfeindlichen Ausschreitungen in Rostock-Lichtenhagen wird vor dem LG Schwerin das Hauptverfahren gegen drei Beteiligte eröffnet. Der Vorsitzende Richter begründete die lange Zeit bis Verhandlungsbeginn mit der Überlastung der Justiz.

24.11.: **Schily übernimmt DFK-Vorsitz**: Bundesinnenminister Otto Schily wird zum Vorsitzenden der im Juli 2001 gegründeten Stiftung Deutsches Forum für Kriminalprävention (DFK) gewählt.

27.11.: **Beobachtung des „Marxistischen Forums" eingestellt**: Der Berliner Innensenator Ehrhart Körting (SPD) gibt bekannt, dass die PDS-Gruppierung nicht mehr vom Berliner Verfassungsschutz überwacht wird. Damit steht von der PDS der Hauptstadt nur noch die „Kommunistische Plattform" unter geheimdienstlicher Beobachtung.

29.11.: **Protestaufruf mit Geldstrafe geahndet**: Das Amtsgericht Ludwigsburg verhängt gegen die Organisation „Gewaltfreie Aktion Atomwaffen Abschaffen" (GAAA) eine Geldstrafe in Höhe von 3.600 DM, weil sie zur Inspektion des Atomwaffenlagers Büchel aufgerufen hatte.

Dies sei eine Aufforderung zum Hausfriedensbruch, so das Gericht, da auch militärisches Gelände betreten werden sollte.

28.11.: **Polizeikommission aufgelöst**: Die Hamburgische Bürgerschaft beschließt mit der Mehrheit von CDU und Schill-Partei die Abschaffung der Polizeikommission. Sie war im September 1998 auf Empfehlung des Untersuchungsausschusses über die Missstände bei der Hamburger Polizei eingesetzt worden und sollte als unabhängige Beschwerdestelle für betroffene BürgerInnen und PolizeibeamtInnen dienen. Erst am Vortag hatte das bundesweit einmalige Gremium seinen dritten und letzten Jahresbericht veröffentlicht, der 136 Beschwerdefälle enthält.

Dezember 2001

09.12.: **Brechmitteleinsatz endet tödlich**: Bei einem Polizeieinsatz im Rechtsmedizinischen Institut in Hamburg wird einem Rauschgifthändler, der 45 Crack-Kügelchen verschluckt hatte, trotz heftiger Gegenwehr gewaltsam ein Brechmittel eingeflößt. Daraufhin erleidet der aus Kamerun stammende Mann einen Herzstillstand und fällt ins Koma. Drei Tage später stirbt er, ohne wieder das Bewusstsein erlangt zu haben. Der designierte neue Polizeipräsident Hamburgs, Udo Nagel, erklärt in einem am 7.1.2002 veröffentlichten Interview, an der umstrittenen Praxis festhalten zu wollen. Am 6.1.2002 wird bekannt, dass der Berliner Innensenator Ehrhart Körting (SPD) die Polizei in der Hauptstadt angewiesen hat, mutmaßlichen Drogenhändlern nicht mehr gegen ihren Willen Brechmittel zu verabreichen. (S. S. 59 ff. in diesem Heft.)

Unschuldiger bei SEK-Einsatz schwer verletzt: Auf der Suche nach einem bewaffneten Mann stürmt ein Sondereinsatzkommando der Polizei bei einem nächtlichen Einsatz im schleswig-holsteinischen Heide irrtümlich eine falsche Wohnung und überwältigt einen anwesenden 60-Jährigen, der einen Beinbruch und Prellungen davonträgt.

11.12.: **Entscheidung über Ausreiseverbote**: Das Berliner Verwaltungsgericht (VG) gibt der Klage eines Globalisierungskritikers statt, dem die Behörden untersagt hatten, zum EU-Gipfel nach Brüssel zu fahren. In zwei anderen Fällen bestätigt das Gericht die Ausreiseverbote, da die Betroffenen in der Vergangenheit an gewaltsamen Aktionen teilgenommen hätten, so die Richter. Insgesamt sollen allein in Berlin 29 angeblich

gewaltbereite Globalisierungskritiker ein Ausreiseverbot zum Zeitpunkt des EU-Gipfels erhalten haben.

12.12.: **„Kalifatsstaat" verboten**: Bundesinnenminister Otto Schily verfügt das Verbot des „Kalifatsstaates", einer Organisation des Islamistenführers und selbst ernannten „Kalifen von Köln" Metin Kaplan. Schily begründet diesen Schritt mit der Gefährdung der inneren Sicherheit. Damit wurde erstmals auf der Grundlage der neuen Anti-Terror-Gesetze, die u.a. den Wegfall des Religionsprivilegs vorsehen, eine extremistische Organisation verboten. Am 17.12. entscheidet das Kölner VG, dass Kaplan nicht sofort ausgewiesen werden darf.

Nachträgliche Sicherungsverwahrung in Bayern beschlossen: Der Bayerische Landtag nimmt mit großer Mehrheit ein Gesetz an, das die nachträgliche Anordnung von Sicherungsverwahrung für besonders gefährliche Straftäter ermöglicht. Als drittes Bundesland nach Baden-Württemberg und Bayern verabschiedet auch Sachsen-Anhalt am 24.2. ein solches Unterbringungsgesetz, durch das rückfallgefährdete Straftäter auch nach Verbüßung ihrer Strafe weiterhin in Haft gehalten werden können.

13.12.: **Einsatz von V-Leuten bei Scientology untersagt**: Das Berliner VG gibt einer Klage der Scientology-Sekte statt und verbietet dem Berliner Verfassungsschutz, sich durch den Einsatz von V-Leuten Informationen über die Organisation zu beschaffen. Ansonsten bleibt die Beobachtung mit nachrichtendienstlichen Mitteln jedoch erlaubt.

14.12.: **Zweites Sicherheitspaket verabschiedet**: Mit den Stimmen der Regierungskoalition und der Union beschließt der Bundestag das Terrorismusbekämpfungsgesetz, das u.a. Pass- und Ausweisregelungen verschärft und die Befugnisse von Polizei, Bundesgrenzschutz und Geheimdiensten drastisch ausweitet. Am 20.12. passiert das Gesetzespaket den Bundesrat und tritt am 1.1.2002 in Kraft.

Prostituiertengesetz gebilligt: Der Bundestag beschließt ein Gesetz, wonach Verträge zwischen Prostituierten und ihren Freiern künftig nicht mehr sittenwidrig sind. Damit können Prostituierte in Deutschland fortan ihre Bezahlung gerichtlich erstreiten. Außerdem erhalten sie Zugang zu den Sozialversicherungen.

17.12.: **Schadensersatzforderungen an Castor-Blockierer**: Es wird bekannt, dass fünf Blockierer des Castor-Atommülltransports eine Scha-

densersatzforderung in Höhe von 166.714,95 DM (85.240 EUR) von der Deutschen Bahn, dem Bundesgrenzschutz und dem Technischen Hilfswerk erhalten haben. Die Demonstranten hatten sich im März 2001 auf der Bahnstrecke Lüneburg-Dannenberg angekettet und konnten erst nach Stunden losgeschnitten werden.

19.12.: **Anketten bei Sitzblockaden als Nötigung eingestuft**: Das Bundesverfassungsgericht (BVerfG) veröffentlicht einen Beschluss, wonach sich Demonstranten, die sich bei Blockadeaktionen anketten, wegen gewaltsamer Nötigung bestraft werden können (Az.: 1 BvR 1190/90 u.a.).

25.12.: **Polizeilicher Todesschuss im mittelfränkischen Leinburg**: Nachdem ein Mann in die Wohnung seiner früheren Partnerin eingebrochen ist, bedroht er die Frau und ihren Freund mit einem Messer und legt Feuer. Später attackiert er die herbeigerufenen Polizisten mit gezücktem Messer, woraufhin einer der Beamten aus rund eineinhalb Meter Entfernung sechs Schüsse abgibt. Der Mann wird in Bauch, Brust und Schultern getroffen und verblutet wenig später.

28.12.: **„Innovations-Zentrums" des bayerischen LKA gegründet**: Der bayerische Innenminister Günther Beckstein teilt mit, dass das „Strategische Innovations-Zentrum" (SIZ) mit Beginn des neuen Jahres seine Arbeit aufnimmt. Aufgabe der Institution, die sich aus Beamten der Kriminalpolizei und wissenschaftlichen Mitarbeitern zusammensetzt, sei die Lieferung umfangreicher Prognosen zu möglichen Kriminalitätsszenarien und neue Ansätze für die Verbrechensbekämpfung.

Januar 2002

01.01.: **Wohnungsverweisung nach Polizeirecht erlaubt:** Nach der Änderung des nordrhein-westfälischen Polizeigesetzes darf die Polizei zum Schutz des Opfers vor „häuslicher Gewalt" den Täter aus der Wohnung verweisen und ihm die Rückkehr bis zu zehn Tagen verbieten.

02.01.: **Zahl der Drogentoten für 2001 veröffentlicht**: Nach einer Umfrage der Nachrichtenagentur ap bei den Bundesländern starben im Jahr 2001 bundesweit mindestens 1.735 Süchtige am Konsum illegaler Drogen. Im Vorjahr waren es noch 2.023 gewesen. Damit ist die Zahl der Rauschgiftopfer erstmals seit drei Jahren gesunken.

09.01.: **Asylstatistik publiziert**: Nach Angaben des Bundesinnenministeriums stellten im Jahr 2001 88.287 Menschen einen Asylantrag, 9.723

(12,4%) mehr als im Vorjahr. Hauptherkunftsländer der Asylsuchenden waren der Irak, die Türkei, Jugoslawien und Afghanistan. Die Anerkennungsquote lag bei 5,3%, rund 19% der Antragsteller wurde darüber hinaus Abschiebeschutz gewährt.

Neues Amt für Eberswalder Polizeipräsidentin: Ein Regierungssprecher des Landes Brandenburg gibt bekannt, dass die Polizeipräsidentin der brandenburgischen Stadt Eberswalde, Uta Leichsenring, im April das neu geschaffene Amt als Landesbeauftragte für das Handlungskonzept „Tolerantes Brandenburg" übernehmen wird. Das Polizeipräsidium
Eberswalde, das Leichsenring seit 1991 führt, wird im Zuge der Polizeireform Ende 2002 aufgelöst. Die Polizeipräsidentin hatte sich in ihrem Amt mit Aktivitäten gegen Rechts bundesweit einen Namen gemacht.

13.01.: **RAF-Mitglied durch Gentest überführt**: Die Bundesanwaltschaft in Karlsruhe bestätigt Presseberichte, wonach elf Jahre nach dem Anschlag auf die Bonner US-Botschaft ein im Fluchtauto gefundenes Haar per Gentest der mutmaßlichen RAF-Terroristin Daniela Klette zugeordnet werden konnte. Klette, nach der seit Jahren gefahndet wird, soll auch an einem Überfall auf einen Geldtransporter in Duisburg 1999 beteiligt gewesen sein.

15.01.: **Wachpolizei in Hessen landesweit eingeführt**: Nach dem erfolgreichen Abschluss der Pilotprojekte in Kassel, Gießen und Frankfurt ordnet der hessische Innenminister Volker Bouffier die Anwerbung von 250 neuen sogenannten Wachpolizisten an, die die Polizeiarbeit vor Ort verstärken sollen. Bis Ende des Jahres soll ihre Zahl auf 360 steigen.

18.01.: **RZ-Mitglied gesteht Attentat**: Acht Monate nach Beginn des Prozesses gegen mutmaßliche Aktivisten der Revolutionären Zellen (RZ) vor dem Berliner Kammergericht gibt Rudolf Schindler seine Tatbeteiligung an einem Sprengstoffanschlag und zwei 1986 und 1987 verübten Schusswaffenattentaten zu. Nach dem Geständnis werden der Angeklagte und seine Frau auf freien Fuß gesetzt.

Deutsche Aufbauhilfe für afghanische Polizei: Das Bundesinnenministerium gibt bekannt, das die Bundesregierung den Wiederaufbau der afghanischen Polizei mit „praktischer Ausbildungs- und Ausstattungshilfe" unterstützen wird. Genaue Zahlen werden noch nicht genannt.

20.01.: **Ermittlungen gegen SEK-Beamte**: Es wird bekannt, dass die Staatsanwaltschaft Bonn gegen acht Beamte eines Sondereinsatzkommandos und weitere zwei Polizisten wegen Körperverletzung im Amt ermittelt. Die Polizisten sollen einen Fliesenleger bei einer Hausdurchsuchung schwer verletzt haben. Einer der Beamten war der Nachbar des Mannes und hatte sich mit ihm zerstritten.

Kirchenasyl wird strafrechtlich überprüft: Der brandenburgische Innenminister Jörg Schönbohm (CDU) erklärt in einer parlamentarischen Anfrage, jeden einzelnen Fall der Gewährung von Kirchenasyl im Bundesland auf seine strafrechtliche Relevanz überprüfen zu lassen. Seit Mitte 1999 bis Dezember 2001 waren dem Innenministerium Brandenburgs sieben Fälle von Kirchenasyl bekannt geworden.

22.01.: **Verhandlungstermine im NPD-Verbotsverfahren ausgesetzt**: Das BVerfG hebt sämtliche fünf Termine zur mündlichen Verhandlung über das Verbot der rechtsextremen Partei auf, nachdem ein Abteilungsleiter des Bundesinnenministeriums den Verfassungsrichtern telefonisch mitgeteilt hatte, dass eine der zum Verfahren geladenen „Auskunftspersonen" der rechtsextremen Partei ein V-Mann des Verfassungsschutzes sei. (S. in diesem Heft S. 76 ff.)

Beschwerde gegen Rasterfahndung erfolgreich: Das LG Berlin gibt der Klage dreier islamischer Studenten statt und erklärt die umstrittene Rasterfahndung für unzulässig. Zu einem gleichlautenden Urteil kommen die Richter des LG Wiesbaden am 7.2.2002. Dagegen hält das VG Mainz die umfassende Datensammlung für rechtens und weist am 18.2. die Klage eines Studenten islamischer Religionszugehörigkeit ab. (S. in diesem Heft S. 69 ff.)

Erstmals Löschung deutscher Porno-Website angeordnet: Das brandenburgische Jugendministerium verfügt die Abschaltung einer uckermärkischen Internetseite wegen Verstoßes gegen den Mediendienstaatsvertrag. Zuvor war der Betreiber erfolglos aufgefordert worden, den Zugang zu den pornografischen Inhalten auf Erwachsene zu beschränken.

23.01.: **Keine Verurteilung eines Polizisten wegen sexueller Beleidigung**: In einem Berufungsverfahren vor dem Gießener LG wird ein 44-jähriger Polizeibeamter vom Vorwurf der sexuellen Beleidigung einer Kollegin freigesprochen. Die Richter sehen zwar belastende Anhaltspunkte, zweifeln aber an der Schilderung der betroffenen Beamtin.

29.01.: **Geheimdienste ohne Parlamentskontrolle**: Es wird bekannt, dass der Verfassungsschutz, der Bundesnachrichtendienst und der Militärische Abschirmdienst in Nordrhein-Westfalen 15 Monate ohne parlamentarische Kontrolle Telefonüberwachungen durchgeführt haben. Nach der Landtagswahl im Mai 2000 hatte es das Düsseldorfer Parlament versäumt, die G 10-Kommission neu zu besetzen. Erst am 19. Dezember 2001 trat die Kontrollkommission zusammen und musste die illegalen Abhöraktionen nachträglich genehmigen. Am 30.1. verabschiedet der Landtag eine Gesetzesänderung, nach der die G 10-Kommission auch nach dem Ende einer Wahlperiode im Amt bleibt, bis der Nachfolgelandtag ein neues Gremium gewählt hat.

30.01.: **Strafbefehl für Polizeidirektor**: Die Berliner Staatsanwaltschaft beantragt für den ehemaligen Chef der AG Rumba (Rumänische Bandenkriminalität) einen Strafbefehl wegen Freiheitsberaubung. Das Verfahren gegen elf weitere Beschuldigte wurde zuvor eingestellt. Die Beamten der „Rumba“ hatten 1999 gegen vier Kollegen vom Landeskriminalamt ermittelt, denen vorgeworfen wurde, von rumänischen Einbrechern bestochen worden zu sein. Der einzige Zeuge der Rumba-Ermittler hatte jedoch gelogen.

Rechtsextremist Roeder verurteilt: Die Staatsschutzkammer des LG Frankfurt/M. verhängt gegen den vielfach vorbestraften Neonazi Manfred Roeder eine zweijährige Freiheitsstrafe ohne Bewährung. Roeder hat sich nach Feststellung des Gerichts mit einem offenen Brief an alle Bundestagsabgeordneten im April 2000 der Verunglimpfung des Staates schuldig gemacht.

Februar 2002

13.02.: **Polizeibeamter begeht Selbsttötung**: Ein Augsburger Polizeihauptmeister erschießt sich in der Nacht mit der Dienstwaffe an seinem Arbeitsplatz. Vorausgegangen war eine Fahrt unter erheblichem Alkoholeinfluss, bei der er in eine Kontrolle geraten war. Die Polizei mutmaßt, dass der Beamte mit einem Dienststrafverfahren rechnete, das zu einer Gehaltskürzung oder Beförderungssperre hätte führen können.

Hund ruft Polizei: Ein allein in einer Kulmbacher Wohnung eingesperrter Hund spielt mit dem schnurlosen Telefon, wählt dabei die 110 und landet in der Einsatzzentrale der Polizei. Nachdem der diensthaben-

de Beamte nur ein lautes „Wauwau“ als Antwort erhält, schickt er eine Streife. Diese trifft zeitgleich mit dem überraschten „Herrchen“ ein.

18.02.: **Polizeilicher Datenzugriff gekappt**: Rund 250 hessische Kommunen verweigern der Polizei wegen eines Gebührenstreits den elektronischen Zugriff auf Einwohnermelde- und Kraftfahrzeugdaten in den drei Gebietsrechenzentren des Landes. Hintergrund ist die Weigerung des Landes Hessen, seit Anfang des Jahres die für die täglich 500 Anfragen anfallenden Gebühren von 20 Cent pro Einwohner zu bezahlen. Die Kommunen wollen jedoch nicht zusätzlich zur Bereitstellung der Daten in ihren Ämtern auch noch die Kosten für die zentrale Datensammlung in den Rechenzentren übernehmen. Am 20.2. werden die Daten auf Anweisung des Innenministers Volker Bouffiers wieder freigegeben.
Abkommen über polizeiliche Zusammenarbeit vereinbart: Bundesinnenminister Otto Schily und sein polnischer Amtskollege Krzysztof Janik unterzeichnen ein bilaterales Abkommen über die Zusammenarbeit der Polizei- und der Grenzschutzbehörden beider Länder in den Grenzgebieten.
Schill durch Haartest entlastet: Das Münchener Institut für Rechtsmedizin erklärt, in der Haarprobe des Hamburger Innensenators Ronald Schill keine Hinweise auf regelmäßigen oder gelegentlichen Kokainkonsum gefunden zu haben. Ein anonymer Zeuge hatte in der ARD-Sendung Panorama behauptet, er habe gesehen, wie sich Schill weißes Pulver auf das Zahnfleisch gerieben habe. Daraufhin entschloss sich Schill zu einem Haartest.

21.02.: **Verfassungsklage der Grünen gescheitert**: Der Bayerische Verwaltungsgerichtshof weist eine Klage der grünen Landtagsfraktion nach einem Sitz im Geheimdienstkontrollgremium des Münchener Landtages ab. Die Richter argumentieren, es sei aus Gründen der Geheimhaltung zu rechtfertigen, dass die parlamentarische Mehrheit die Zahl der Mitglieder für das Gremium auf fünf Personen beschränkt habe. Zudem habe das BVerfG die Nichtberücksichtigung einzelner Fraktionen für rechtens erklärt.

25.02.: **Abbau des Nato-Drahtes in Gorleben**: Das Bundesamt für Strahlenschutz ordnet die Entfernung des Nato-Drahtes und der Wasserwerfer von der Umfassungsmauer des geplanten Endlagers Gorleben an. Damit will die Behörde nach eigener Aussage zum 25. Jahrestag des

Endlagerstandortes Gorleben „ein sichtbares Zeichen der Deeskalation setzen."

Andrea Böhm studiert Politikwissenschaft an der FU Berlin und ist Redaktionsmitglied von Bürgerrechte & Polizei/CILIP.

Literatur

Zum Schwerpunkt

Die Befürchtung, dass aus den neuen Kommunikationstechnologien neue Sicherheitsgefahren und neue Schwierigkeiten für die Strafverfolgungsbehörden resultieren, kennen wir aus der Diskussion über die Handy-Überwachung in der ersten Hälfte der 90er Jahre. Wenige Jahre später sind nicht die Straftäter, die sich mit fremden Handys der Polizei entziehen, das Problem, sondern die mobile Telefonie ist zu einer zusätzlichen Überwachungsquelle geworden: Sie ermöglicht nicht allein das Abhören, sondern erlaubt gleichzeitig die Identifizierung von Telefonanschlüssen und die Ortung und Verfolgung der Telefonierenden. Die Wandlung vom angeblichen Sicherheitsverlust zum umfassenderen Überwachungsinstrument steht prototypisch für die realen „Entwicklungschancen" des Telekommunikationszeitalters: Die neuen Informationsfreiheiten machen die BürgerInnen vermehrt zum Objekt staatlicher (und privatwirtschaftlicher) Kontrolle. Dank der neuen Technologien geschieht diese Kontrolle unmerklicher für die Überwachten, sie gerät umfassender – neben den Inhalten werden die äußeren Umstände der Kommunikation überwacht –, und sie unterliegt einem technologisch bedingten schnellen Wandel, der Erweiterungen staatlicher Eingriffsmöglichkeiten nach sich zieht. Insofern gibt auch die Literatur über die neuen Überwachungspraktiken nur eine Momentaufnahme, die teilweise heute schon überholt ist. Wir beschränken uns im Folgenden nur auf wenige Beiträge, die die polizeiliche und geheimdienstliche Telekommunikationskontrolle (vornehmlich in Deutschland) betreffen.

Schulzki-Haddouti, Christiane (Hg.): *Vom Ende der Anonymität. Die Globalisierung der Überwachung, Hannover 2000 (Heise Verlag), 188 S., EUR 15,–*
Im Zentrum dieses 2001 in einer aktualisierten Fassung erschienenen Sammelbandes aus dem Umfeld des Online-Magazins „Telepolis" steht die Entwicklung der internationalen Überwachungsgemeinschaft. Nach einem Überblick des norwegischen Kriminologen Thomas Mathiesen

über die „Globalisierung der Überwachung“ folgen Beiträge über die Kontrollpotentiale auf EU-Ebene (Europol sowie die unter dem Stichwort „Enfopol“ bekannt gewordenen Bemühungen grenzüberschreitender Kommunikationskontrolle im Rahmen der Rechtshilfe). Mehrere Beiträge beschäftigen sich mit dem von der US-amerikanischen National Security Agency betriebenen und von mehreren westlichen Staaten unterstützten Echelon-System, mit dem weltweit Kommunikationsströme (von Satellitenübertragungen bis zu Unterseekabeln) überwacht werden. Für die deutsche Entwicklung ist der Beitrag von Erich Schmidt-Eenboom von Interesse, in dem die Entwicklung und Funktionsweise der Funkspionage des Bundesnachrichtendienstes beschrieben wird. In ganz anderer Weise ist der Beitrag von Detlef Nogala lesenswert, weil er zeigt, wie breit das technologisch machbare Überwachungsspektrum mittlerweile geworden ist. Die technologische Entwicklung vervielfache nicht nur die Kontrollmöglichkeiten, sondern – so die ernüchternde Diagnose – sie erhöhe auch deren Akzeptanz.

Germann, Michael: *Gefahrenabwehr und Strafverfolgung im Internet (Schriften zum Öffentlichen Recht, Bd. 812), Berlin 2000 (Duncker & Humblot), 757 S., EUR 96,–*

Eine Bestandsaufnahme der „staatlichen Möglichkeiten“ zu Gefahrenabwehr und Strafverfolgung im Internet ist Anliegen dieser dickleibigen juristischen Dissertation. Neben einer Untersuchung des Polizei- und Strafprozessrechts betrachtet der Autor – wenn auch eher am Rande – die Befugnisse der Geheimdienste für die Informationsbeschaffung im Internet. Die Rechtsentwicklung ist dabei bis Juni 1999 berücksichtigt.

Bevor Germann daran geht, die polizei- und geheimdienstlichen Maßnahmen im weltweiten Datennetz auf ihre Rechtsgrundlagen zu überprüfen, erfährt der/die LeserIn zunächst vergleichsweise anschaulich etwas über die Funktionsweise des Internet, die verschiedenen Dienste (WWW, E-Mail, Chat etc.) und welche (Multi-Media-)Gesetze darauf anwendbar sind. Jeweils eigene Kapitel sind den technischen Möglichkeiten und Grenzen der Gefahrenabwehr und Strafverfolgung im weltweiten Datennetz sowie den Pflichten der Internet-Provider und Inhalteanbieter gewidmet. Schließlich analysiert der Autor – nach Gefahrenabwehr und Strafverfolgung getrennt – verschiedene Ermittlungsmaßnahmen, angefangen bei der Sperrung von Internetangeboten über verdachtsunabhängige Internet-Streifen und Auskunftsverlangen über Nut-

zerdaten bis zur (verdeckten) Informationsbeschaffung durch Teilnahme an der Internetkommunikation und Abhörmaßnahmen.

Im Ergebnis sieht Germann „erhebliche Vollzugsdefizite“ bei Polizei und Geheimdiensten. Diese seien aber weniger auf rechtliche Befugnislücken zurückzuführen als auf technische Probleme wie z.B. Verschlüsselung, Anonymisierung oder Verschleierung der Identität im Internet. Diese Analyse ist nur konsequent, da der Autor Polizei- und Strafprozessrecht an vielen Stellen „eingriffsfreundlich“ auslegt und daher kaum Schranken sieht. Trotz einiger Einschränkungen ist das Buch gut geeignet, sich gründlich mit der Problematik auseinander zu setzen.
(Martina Kant)

Deutsches Polizeiblatt 19. Jg., 2001, H. 4 (Schwerpunkt: Internet)
Das Schwerpunktheft informiert in kurzen Beiträgen über die wichtigsten Aspekte des Themas „Polizei und Internet“: Kriminalität im Internet (insbes. Politischer Extremismus), „Befugnisse und Grenzen der Ermittlungsbehörden“, kriminalpolizeiliche Ermittlungen und anlassunabhängige Streifen im Internet, „Tatmedium E-Mail“ sowie das Netz als Medium polizeilicher Außendarstellungen. Das Heft gibt insgesamt einen ersten Einblick in die Praxis der polizeilichen Internetüberwachung sowie deren rechtliche und technische Schwierigkeiten. Mitunter helfen die Hinweise jedoch kaum weiter, etwa wenn in der zusammenfassenden „Checkliste“ vermerkt wird: „Das Internet tangiert fast alle Delikte des Strafgesetzbuches“ oder: „Finden und Sichern digitaler Spuren erfordert technischen Sachverstand.“

Bär, Wolfgang: *Auf dem Weg zur „Internet-Polizei“?, in: Bäumler, Helmut (Hg.): Polizei und Datenschutz, Neuwied, Kriftel 1999, S. 167-187*
Bärs Ausführungen gelten zum einen den rechtlichen Grundlagen der Strafverfolgung im Internet, zum anderen beleuchtet er das Internet als Instrument polizeilicher Fahndung. Obwohl der Beitrag noch keine drei Jahre alt ist, ist er von der Rechtsentwicklung längst überholt: Grundlagen für die Fahndung wurden durch das Strafverfahrensänderungsgesetz 1999 in die Strafprozessordnung aufgenommen. Und die polizeilichen Überwachungsbefugnisse der Telekommunikation sind im Dezember

2001 durch die neuen §§ 100g und 100h der StPO und die jüngst erlassene Telekommunikationsüberwachungsverordnung erweitert worden.

Weichert, Thilo: *Cyber-Crime-Bekämpfung und Datenschutz, in: Datenschutz-Nachrichten 24. Jg., 2001, H. 2, S. 5-15*
Aus datenschützerischer Perspektive diskutiert Thilo Weichert die Probleme des Cybercrime und deren staatlicher Verfolgung. Nach einem kurzen Blick auf die Besonderheiten der Internet-Kriminalität werden die nationalen und internationalen Regulierungen und Kontrollbefugnisse dargestellt. Auf die deutsche Situation bezogen, diskutiert Weichert den damaligen Entwurf der Telekommunikations-Überwachungsverordnung. Darüber hinaus werden einige (weiterhin) offene Fragen angesprochen, wie z.B. die Ermittlungstätigkeit Verdeckter Ermittler im Netz. Der Zugriff der Sicherheitsbehörden auf personenbezogene Informationen müsse an „strenge rechtliche Voraussetzungen" gebunden werden, und den „Kontrollforderungen der Sicherheitsbehörden" könne „nicht ohne Etablierung rechtsstaatlicher Kontrollverfahren nachgegeben werden."

Hetzer, Wolfgang: *Neuregelung der Telekommunikationsüberwachung, in: Kriminalistik 55. Jg., 2001, H. 5, S. 347-354*
Der Beitrag des Ministerialrats im Bundeskanzleramt ist eine Erläuterung des damals noch in der parlamentarischen Beratung befindlichen neuen G 10-Gesetzes, das erforderlich geworden war, nachdem das Bundesverfassungsgericht mehrere Bestimmungen für verfassungswidrig erklärt hatte, mit denen die Abhörbefugnisse des Bundesnachrichtendienstes ausgeweitet worden waren. Hetzers Aufsatz steht für jene Art von Literatur, mit der die Beteiligten die Gesetzgebungsmaschinerie mit großer rechtsstaatlicher Semantik legitimieren. So wird der Umstand, dass Daten aus der Telekommunikationsüberwachung nur an diejenigen Stellen übermittelt werden dürfen, die diese Daten zur Erfüllung ihrer Aufgaben benötigen, als Beschränkung interpretiert. Wer lesen will, wie die Ausdehnung der Überwachung begründet und in entgrenzende juristische Formulierungen gegossen wird, der/die sollte diese Erläuterungen des mittlerweile in Kraft getretenen Abhörgesetzes gründlich lesen.

Zimmermann, Georg: *Staatliches Abhören, Frankfurt am Main, Berlin, Bern u.a. 2001 (Peter Lang), 327 S., EUR 50,10*
Die Verrechtlichung des „Großen Lauschangriffs" vor wenigen Jahren, der Rechtsstreit über das Abhören durch den Bundesnachrichtendienst, das jährliche steigende Ausmaß der polizeilichen Telefonüberwachung – die Zeit war eigentlich schon lange reif für eine Gesamtsicht „staatlichen

Abhörens“. Georg Zimmermann hat mit seiner juristischen Dissertation einen wichtigen Beitrag zu einer solchen Bilanz vorgelegt. Im Hauptteil der Untersuchung schildert er in chronologischer Folge die „Entwicklung der gesetzlichen Befugnisse zum hoheitlichen Abhören von Gesprächen in der Geschichte der Bundesrepublik“. Innerhalb der drei vom Autor festgestellten Entwicklungsphasen (bis zu den Notstandsgesetzen, die 70er und 80er Jahre, und die 90er Jahre) werden jeweils die strafprozessualen, die polizeirechtlichen sowie die geheimdienstlichen und für die 90er Jahre zollrechtlichen Abhörbefugnisse „im Detail referiert“.

Der Horizont des Buches geht jedoch über diese rein beschreibende Zielsetzung – für sich schon ein lobendes und mühevolles Unterfangen – hinaus: Zimmermann interessiert sich für die Entwicklung der Abhörnormen, weil er vermutet, dass das im Laufe der Jahrzehnte dichter, vielfältiger und unübersichtlicher gewordene Normengeflecht nicht zu mehr, sondern zu weniger rechtsstaatlicher Begrenzung geführt hat. Diese These belegt die Studie nachdrücklich: Zum einen wird an der strafprozessualen Norm zur Telefonüberwachung (§ 100a StPO) die inflatorische Ausweitung der Einsatzgebiete nachgezeichnet, die nicht allein durch die Aufnahme neuer Katalogtaten entsteht, sondern durch die Ausdehnungen, die jene Taten im Bereich des Strafrechts erfahren. Diese direkten und indirekten Erweiterungen sind, so Zimmermann, nicht durch die Schwere der Taten oder kriminalistische Argumente bestimmt, sondern durch politische Tagesaktualitäten. Wenn der Gesetzgeber nicht mehr weiter weiß, so darf man dieses Argument zusammenfassen, dann erweitert er die Möglichkeiten zum Abhören.

Zum anderen bieten die verschiedenen Eingriffsnormen des Abhörrechts Möglichkeiten, etwa die Bestimmungen der Strafprozessordung zu umgehen, indem Erkenntnisse der Nachrichtendienste, des Zollkriminalamtes oder polizeirechtlich gewonnene Abhördaten in das Strafverfahren eingeführt werden. Um die Bedeutung des Abhörens für die Strafverfolgung erfassen zu können, reiche der Blick in die Strafprozessordnung nicht aus: „vielmehr stellt ein paralleles Verfahrenssystem häufig entsprechende Befugnisse unter erleichterten verfahrensrechtlichen Voraussetzungen zur Verfügung“.

Internetquellen

Cryptome: http://cryptome.org
Eine wahre Fundgrunde für „classified" Dokumente aus den verschiedensten Bereichen. Stichworte: Echelon, ETSI, Enfopol; siehe auch die Dokumente zur Telekommunikationsüberwachung: http://cryptome.org/e-spy-telecom.htm

Privacy International: http://www.privacyinternational.org
Bürgerrechtsorganisation mit Büros in London und Washington, aus dem Umfeld der Organisation wurden die Big-Brother-Schnüffelpreise einberufen

Quintessenz: http://www.quintessenz.org
„Verein zur Wiederherstellung der Menschenrechte im Informationszeitalter"

Futurezone: http://futurezone.orf.at
Online-Magazin des ORF, Chefredakteur ist Erich Moechel, Autor der ETSI-Dossiers

Telepolis: http://www.heise.de/tp
Magazin der Netzkultur, veröffentlicht täglich Texte zur Netzpolitik, Überwachungseuropa u.a.; siehe dort auch zu den Enfopol-Papieren: http://www.heise.de/tp/deutsch/special/enfo/

Sonstige Neuerscheinungen

Lisken, Hans; Denninger, Erhard (Hg.): *Handbuch des Polizeirechts, 3., neubearbeitete und erweiterte Auflage, München 2001 (Verlag C.H. Beck), 1279 S., EUR 112,–*

Nach fünf Jahren und um fast 300 Seiten angewachsen ist im Herbst vergangenen Jahres die dritte Auflage von „Lisken-Denninger" erschienen. Mittlerweile ist das „Handbuch des Polizeirechts" als Standardwerk kritischer Polizeirechtskommentierung etabliert. Die aktuelle Ausgabe ist um das Kapitel „Gefahrenabwehr durch Ordnungsverwaltung" erweitert, in dem die materiellen Polizeiaufgaben des Ausländer-, Bau-, Gewerbe-, Waffen- und Umweltrechts dargestellt werden. Darüber hinaus wird den Entwicklungen von Polizeirecht und -praxis der letzten fünf Jahre Rechnung getragen. Dazu zählen die Videoüberwachung und die „ereignis- und verdachtsunabhängigen" Identitätsüberprüfungen. Die Ausführungen zur Schleierfahndung sind von 2 auf 12 Seiten angewachsen. „Vieles spricht dafür", so der Autor nach der Würdigung der geltenden Bestimmungen, „daß die neuen Kontrollbefugnisse wegen Verstoßes gegen den Verhältnismäßigkeitsgrundsatz verfassungswidrig sind" (S. 414). Auf die weitere Europäisierung der Polizeiarbeit reagiert das Handbuch durch längere – und ernüchternde – Ausführungen zum Rechtsschutz gegenüber „Europol-Eingriffen (S. 994-1004) sowie mit einem im Umfang

mehr als verdoppelten Abschlusskapitel über die „Polizeiliche Zusammenarbeit in Europa“. In diesem Teil wird nicht nur das unübersichtliche Geflecht europäischer Polizeikooperation und Institutionen vorgestellt – von den direkten Kooperationen mit den Nachbarstaaten bis zur Praxis nach den Schengener Verträgen oder der Arbeit von Europol. Gleichzeitig werden immer wieder die rechtsstaatlich problematischen Elemente benannt, die aus der Europäisierung der Polizei resultieren: Rechtsschutz gegen Registrierung im Schengener Informationssystem, Immunität für Europol-Beamte, die notorischen Kontrolldefizite gegenüber den Praktiken und Instanzen europäischer Innerer Sicherheitswahrung. Das Handbuch bleibt ein aktueller, kritischer und unverzichtbarer Beobachter der rechtlichen und institutionellen Veränderungen des „Systems Innerer Sicherheit“ in Deutschland und Europa.

Möllers, Martin H.W. (Hg.): *Wörterbuch der Polizei, München 2001 (Verlag C.H. Beck), 2001 S., EUR 92,–*

Natürlich kann man dieses Nachschlagewerk nicht angemessen besprechen: 50 AutorInnen, über 10.000 erläuterte Fachbegriffe auf gut 2.000 dicht beschriebenen Seiten. Das weite Spektrum, das das Wörterbuch abdeckt, reicht von rechtlichen bis institutionellen, von naturwissenschaftlichen bis kriminologischen, von politischen bis polizei-praktischen Begriffen. Natürlich stellt dieses Buch eine hervorragende Quelle für alle dar, die sich schnell und kompetent über „Polizei“ und Sachverhalte, die in irgendeiner Weise polizeilichen Bezug haben, informieren wollen. Die Vielzahl der Begriffe, die Aufnahme von Synonymen, die vielen Querverweise sowie die Angabe wichtiger Literatur machen aus dem „Wörterbuch“ mehr als ein schlichtes Nachschlagewerk. Und natürlich lassen sich Einträge unterschiedlicher Qualität in dem Band finden. Das gilt vor allem im Hinblick auf eher kritische oder bürgerrechtliche Positionen. So fördern einige Leseproben durchaus Defizite zu Tage: Im Beitrag über Pfefferspray wird zwar auf eine österreichische Untersuchung verwiesen, aber Hinweise auf angelsächsische Studien oder die Berichte von amnesty international fehlen. Die Verve, mit der die Befugnis zum Todesschuss gefordert oder die Rechtswidrigkeit des Kirchenasyls konstatiert wird, fehlt leider an anderer Stelle, etwa bezogen auf die Wachstumsraten bei der Telefonüberwachung oder hinsichtlich der Rechtsprobleme verdeckter Polizeiarbeit, die zwischen den Stichworten „Verdeckter Ermittler“ und „nicht offen ermittelnder Polizeibeamter“ verharmlost statt auf

den Punkt gebracht werden. Auch dass das „Wörterbuch“ unter dem Stichwort „Organisierte Kriminalität“ über drei Spalten Deliktsfelder, Paragrafen und Zahlen aus dem Lagebild auflistet, aber die einzige Monografie nicht zu kennen scheint, die den polizeilichen Umgang mit OK thematisiert, deutet darauf hin, dass das Nachschlagwerk mehr informieren als kritisch informieren will. Wer das Buch jedoch zum eigenen Nachdenken und Forschen nutzen wird, dem oder der wird es von großem Nutzen sein.

Witzstrock, Heike: *Der polizeiliche Todesschuss, Frankfurt am Main, Berlin, Bern u.a. 2001 (Peter Lang), 209 S., EUR 35,30*
Mußgnug, Friederike: *Das Recht des polizeilichen Schußwaffengebrauchs, Frankfurt am Main, Berlin, Bern u.a. 2001 (Peter Lang), 287 S., EUR 45,50*
Die beiden juristischen Dissertationen zum Recht des polizeilichen Schusswaffengebrauchs könnten in ihren Schlussfolgerungen kaum unterschiedlicher sein. Die breitere, auf das gesamte polizeiliche Schusswaffengebrauchsrecht angelegte Untersuchung Mußgnugs diagnostiziert am Beispiel des nordrhein-westfälischen Polizeirechts erhebliche Regelungslücken. Zum einen hält sie die allgemeinen Voraussetzungen für den Schusswaffeneinsatz gegen Personen für unzureichend. Statt den Verweis auf Verbrechen und Vergehen, die das geltende Recht enthält, schlägt sie eine Formulierung vor, die auf eine Ausweitung der Befugnis hinausläuft; etwa indem das Schießen auf Personen erlaubt werden soll, um „die unbefugte Zerstörung ... eines besonders gekennzeichneten Kulturgutes von nationaler Bedeutung“ zu verhindern (S. 248). Auch im Hinblick auf den „finalen Rettungsschuss“ plädiert die Autorin für eine explizite polizeirechtliche Regelung. Zwar sei der gezielte Todesschuss auch in NRW zulässig, aber es sei eine Frage rechtsstaatlicher Klarheit, der Fürsorgepflicht gegenüber den PolizistInnen und der Ehrlichkeit, den mit an Sicherheit grenzender Wahrscheinlichkeit tödlich wirkenden Schuss im Polizeigesetz zu regeln, statt – wie in NRW – ihn in einer Verwaltungsvorschrift zu verstecken (S. 92).

Während nach der Auffassung von Mußgnug die Notwehrrechte als rechtliche Fundierung des gezielten Todesschusses ausscheiden, sieht Witzstrock die Bestimmungen des Strafgesetzbuches über Notwehr und Nothilfe als ausreichende und angemessenere Rechtsgrundlage für polizeiliche Todesschüsse an. Die verfassungsrechtlichen Vorgaben erlaubten

durchaus, den „finalen Rettungsschuss“ im Polizeirecht zu verankern. Mit einer Norm, die das staatliche Töten auf Befehl legalisiere, würde jedoch rechtspolitisch ein falsches Signal gesetzt. Dass das Notwehrrecht keine Befugnis zur Gewaltanwendung enthalte und somit die Anordnung eines Todesschusses ausschließe, sei angemessen: Denn nach dem Verhältnismäßigkeitsprinzip könne immer nur der Schütze entscheiden, ob ein wohl tödlich wirkender Schuss das einzige Mittel bleibe. Von dessen persönlicher Verantwortung für sein Handeln werde er auch nicht durch eine polizeirechtliche Ermächtigung befreit.

Beiden Arbeiten ist gemeinsam, dass sie von der Wirklichkeit polizeilichen Schusswaffengebrauchs nur rudimentär Kenntnis nehmen. Mußnug hätte dann feststellen müssen, dass die rechtlichen Lücken bislang weder negative noch positive Auswirkungen für die Praxis gehabt haben. Und Witzstrock hätte ihr Argument noch stärker machen können, dass nicht das Recht, sondern die polizeiliche Ausbildung und Einsatzlehre – vielleicht auch allgemeinere politische Entwicklungen – darüber entscheiden, wann und wie es zu gezielten Polizeischüssen auf Menschen kommt. Wer realisiert, dass der „finale Rettungsschuss“ eine seltene Ausnahme unter den polizeilichen Todesschüssen darstellt, der/die wird feststellen müssen, dass die Auseinandersetzungen um die Rechtsgrundlagen von den Problemen polizeilicher Gewaltanwendung eher ablenken. (sämtlich: Norbert Pütter)

Gleß, Sabine; Grote, Reiner; Heine, Günter (Hg.): *Justitielle Einbindung und Kontrolle von EUROPOL, Freiburg im Breisgau 2001 (edition iuscrim), 2 Bände, 694 u. 638 S.*, EUR 66,50

Die Arbeit von EUROPOL unterliegt gegenwärtig keiner Kontrolle. Weder die datenverarbeitenden Tätigkeiten noch die Beteiligungen an gemeinsamen Ermittlungsteams mit den Polizeien der Mitgliedstaaten können von Gerichten überprüft werden. Auch die Parlamente werden nur vorbehaltlich der Geheimhaltungspflicht informiert, unmittelbare Einwirkungsbefugnisse oder Kontrollmöglichkeiten haben sie nicht. Das vorliegende Gutachten wurde im Auftrag des Bundesjustizministeriums vom Max-Planck-Institut für ausländisches und internationales Strafrecht erstellt. Es sollte prüfen, inwieweit eigene Ermittlungsbefugnisse von EUROPOL, wie sie nach Art. 30 Abs. 2 des Europäischen Unionsvertrages vorgesehen sind, gerichtliche und parlamentarische Kontrolle notwendig machen.

Das Verhältnis von Staatsanwaltschaft und Polizei in den Mitgliedstaaten bildet einen Schwerpunkt des Gutachtens. Denn die Staatsanwaltschaft hat während eines laufenden Ermittlungsverfahrens eine Weisungsbefugnis gegenüber den ermittelnden Polizeibeamten. Die Errichtung einer entsprechenden europäischen Behörde könnte insofern eine Einbindung von EUROPOL bedeuten. Die Diskussionsansätze hierzu werden von den Verfassern ausführlich besprochen und kritisch betrachtet. Daran zeigt sich, dass die tatsächliche Errichtung noch nicht absehbar ist. In Bezug auf die demokratische Einbindung von EUROPOL monieren die VerfasserInnen neben einer stärkeren parlamentarischen Kontrolle, vor allem die Immunität der EUROPOL-Beamten, die bei einer Ausweitung der Kompetenzen aufgehoben werden müsse.

Ein weiterer Schwerpunkt der Arbeit liegt in der Beurteilung der Beweisverwertung bei Ermittlungsverfahren, die in mehreren Staaten verlaufen. Die Uneinheitlichkeit nationaler Verfahrensregeln kann dazu führen, dass Beweise nach den Vorschriften vor Ort erhoben wurden, diese aber im Widerspruch zu den Landesvorschriften stehen, wo das Gerichtsverfahren stattfindet und die Beweise verwertet werden. Die Gefahr ist offenkundig, dass derart Rechte von Beschuldigten nach und nach ausgehöhlt werden. Ein europäisches Verfahrensrecht, welches hier Abhilfe schaffen könnte, hat noch nicht einmal Konturen angenommen.

Das Gutachten zeigt damit wesentliche Probleme auf und macht deutlich, dass eigene Ermittlungsbefugnisse von EUROPOL grundlegende Strukturveränderungen der europäischen Innen- und Justizpolitik notwendig machen. Damit äußern die VerfasserInnen auch offen Kritik an den bestehenden Zuständen, die vor allem den Bereich der Datenverarbeitung betreffen. Hier kann EUROPOL frei von Datenschutzbestimmungen und externer Kontrolle fast jede Form der Daten verarbeiten und vor allem mit weiteren Institutionen austauschen.

Ein Manko an dem Gutachten ist, dass die einzelnen Länderberichte aufgrund nicht aufeinander abgestimmter Gliederungen nur schwer zu vergleichen sind. Das sollte das Justizministerium nicht hindern, sich dieses Gutachten zu Herzen zu nehmen.
(Olaf Griebenow)

Summaries

Cybercrime – the future of electronic surveillance

by Albrecht Funk

The much-recited mantra that cybercrime is an abuse of the internet is misleading. Behind the moralising crusades against child pornography and „Islamic terrorism“ are interest coalitions of private and public actors, who are trying to create the future order of public rights and public wrongs in their image and at any cost.

Surveillance of telecommunications – who is allowed to do what and when?

by Norbert Pütter

In Germany, the police, customs and the three security services have legal powers to intercept telecommunications. An increasing role is now being played by law enforcement powers to collect and analyse traffic data.

Surveillance of mobile phone communication

by Björn Gehrke

Compared with the traditional mainline telephones, the mobile telephone allows for a whole new plethora of surveillance possibilities – from the collection of traffic data over the direction bearing and position finding via GPS to the use of the IMSI-Catcher. Legislation and court decisions have legitimised these new instruments of surveillance.

“Internet-patrols” of police and security services

by Martina Kant

In 1995, the Bavarian police force began searching the internet for criminal content, without any concrete grounds for suspicion. By now, the Federal Crime Police Authority and the security services surf the internet for illegal and unconstitutional contents as well. This article describes the investigation methods and raises questions about the legal basis for internet surveillance.

“Vorsprung durch Technik”

by Erich Moechel and Nick Lüthi

Since 1992, EU Law Enforcement Agencies as well as the FBI have formulated and presented their International User Requirements. Parallel to this, a working group of the European Telecommunications Standards Institute has developed interfaces, which basically allow for the automatic surveillance of all telecommunication networks.

What will happen with the traffic data?

by Tony Bunyan

According to an EU Directive from 1997, traffic data resulting from any telecommunication has to be deleted as soon as it is not needed for billing purposes anymore. In revising this Directive, the EU Council want to abolish this principle. Providers are now supposed to retain this data and grant law enforcement agencies access to it. So far, the European Parliament is resisting this move.

Echelon and the failure of the European Parliament

by Heiner Busch

The report by the EP Echelon Committee has confirmed the existence of the surveillance apparatus. But its conclusions are disastrously unpolitical. They hold that security services‘ signals intelligence activities (SIGINT activities) are covered by the European Convention of Human Rights, if they have a legal basis and are controlled by Parliament. The EP Echelon Committee supports the closer co-operation between security services of EU Member States.

The Cybercrime Convention

by Sönke Hilbrans

On 23 November 2001, the Council of Europe member states as well as Canada, the US, Japan and South Africa, signed the Cybercrime Convention in Budapest. Amongst other things, the Convention aims at creating international minimum standards for the collection of traffic data. At the normative level, the Convention further erodes the protection of basic rights and human rights.

About torture

by Fredrik Roggan

On 9 December 2001, a 19-year-old Cameroonian died as a consequence of the forceful use of emetic by the police. The Hamburg police force is not the only one that regularly enforces the use of such highly dangerous substances, with the justification of the suspicion of drug smuggling in the body or of a person having swallowed them when police arrives.

Terrorism Act in force

by Norbert Pütter

The Parliament only needed six weeks to put the „Law on the Fight against International Terrorism“ into force. Those who profit from the law are particularly the security services, but also the Federal Crime Police Authority. The rights of refugees and migrants are, yet again, curtailed.

Computerised profile searches

by Heiner Busch

The computerised profile searches for possible members of the „al Q‘aida terror network“, which started at the end of September last year, in particular targeted the foreign population. Courts in two different *Länder* have now declared the police operation illegal. Although masses of personal data of non-suspects have been collected during these computerised profile searches, it was clear from the start that the operation could not be expected to produce „successes“.

The poor constitution

by Wolf-Dieter Narr

In January, the press reported that five NPD members, who were supposed to give evidence in front of the Federal Constitutional Court for the NPD trial, which considers the Government‘s application for a ban of the right-wing party, were informants of Germany‘s internal security service, the *Verfassungsschutz*. The court however, had not been informed about this fact. The only sensible conclusion to this case would be the abolition of the internal security service.